7.5.11   FCU Menu

Fig 48:   FCU Menu web page

This screen is accessible to Read, Write and Administrator user levels.

The FCU Menu lists all the field units in address order (which may not be the same as the order in which they are connected together on the wired loop).

For each address, the Tag name and Type of field unit is listed. Field unit types are described in section 7.5.7. The Network column shows which option module network each actuator is connected to; this will be Pakscan 2 for the 2-wire loop option module and Wireless for the wireless option.

The next two columns show critical alarm conditions that will prevent remote control of the actuator. An Alarm present will generally prevent operation, whilst Comms Fail indicates that the actuator is no longer in communication with the field network.

The final column has Navigation controls to the individual FCU screens.

Controls - Available to all user levels

FCU Control   : Click here to show the selected FCU individual control panel web page. The different types of devices each have different screens and only the relevant data and controls for each type are included on the screen, together with a picture identifying the type of device.

When not in communication the screen may still be visited, but the actuator picture will have a large red cross over it to show that a problem exists.

7.5.12   FCU Control – IQ / IQT Actuator
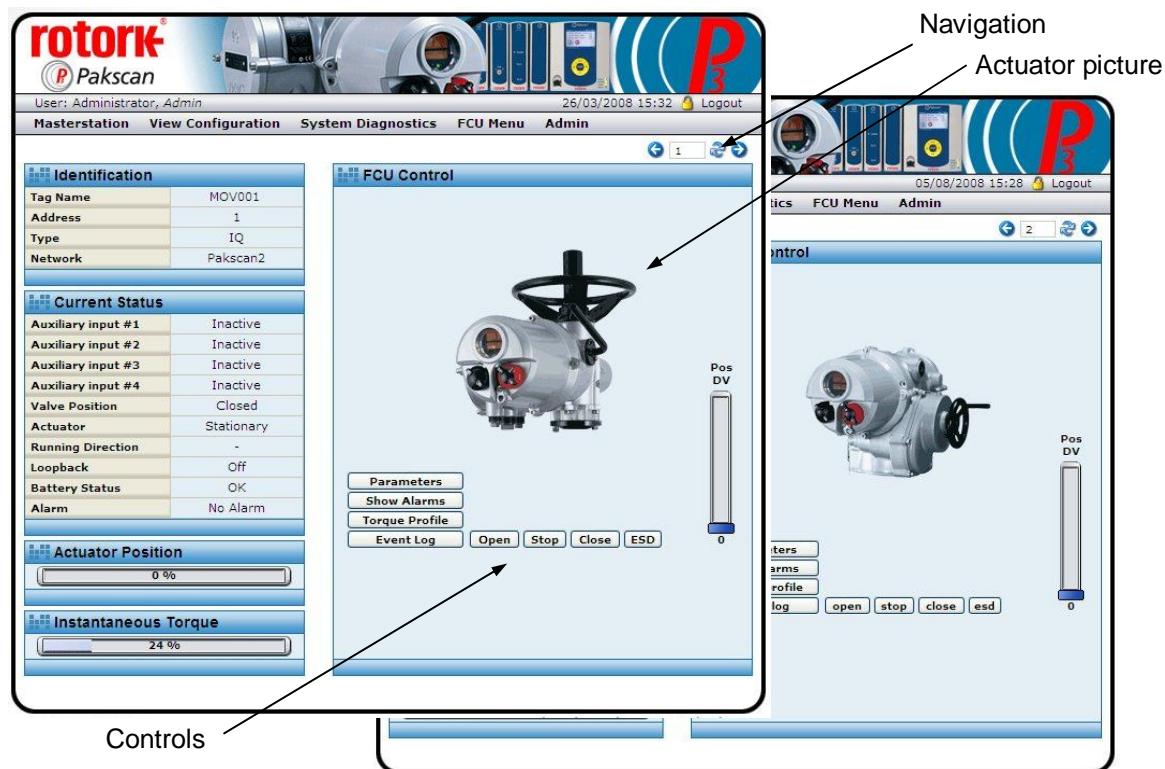
Fig 49:   IQ and IQT actuator FCU Control web pages

This screen is accessible to Read, Write and Administrator user levels.

The IQ and IQT control screens are similar and show a picture to identify the actual type of actuator at this FCU address.

The FCU Control screen shows a control and status page for the selected field unit and actuator. The screen has information relating to the device, its current condition and system parameters. It also includes the ability to change the actuator's position by means of the control buttons. When not in communication the screen may still be visited, but the picture has a large red cross over it to show a lack of communication.

Navigation

Navigation between the field units is either by returning to the previous screen, or by using the navigation buttons on this screen. Entering an address directly in the 'Address' box and clicking Refresh moves directly to the selected field unit.

Identification

    Tag name   : Identification tag given for this device.

    Address   : Network address.

    Type   : Shows the identified actuator type as IQ or IQT.

    Network   : The network to which this device is connected (Pakscan 2 for 2-wire loop).

Current Status

    The real-time status of the actuator is listed in this pane on the screen:

    Auxiliary Input   : Active or Inactive, shows the status of the input.
    1 to 4

    Valve Position   : Current position, Closed, Open or Stopped Mid Position.

    Actuator   : Moving or Stationary.

    Running direction : Opening or Closing.

    Loopback   : Off or On.

    Battery Status   : OK or Low.

    Alarm Status   : No Alarm or Alarm.

Actuator Position

    A bar graph shows the current actuator analogue position between 0 (closed) and 100% (open).

Instantaneous Torque

    A bar graph shows the current torque value between 0 and 120% of actuator rated torque.

FCU Control web page Controls

Parameters (2-wire loop Field unit) - Available to all user levels

    Close pop-up
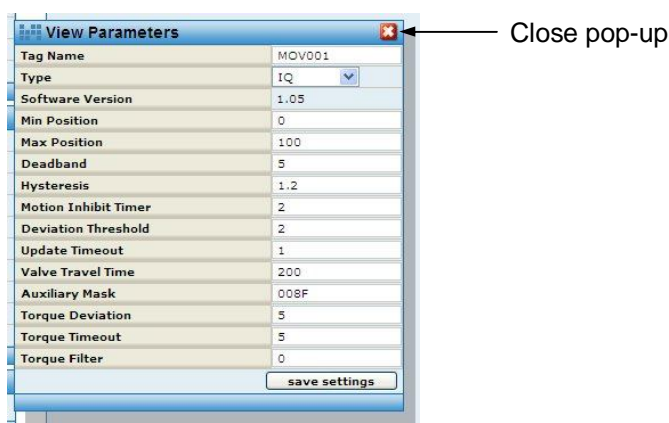
Fig 50:   *Wired IQ / IQT Parameters pop-up*

    Pop-up screen shows the settings for all the parameters relating to the IQ / IQT actuator field unit. For users with Administrator level rights, the values can be edited and, for later version field units, the type of actuator can be modified. The parameters are used to determine the way in which the actuator responds to commands and reports data. Information on how to set

Controls

these fields is contained in the actuator field unit manuals. This screen is used for changing the Tag Name.

Controls

Save Settings   :   Edited fields may be saved to the FCU; accessible by **Administrator** level users only.

Show Alarms (2-wire loop Field unit) - Available to all user levels
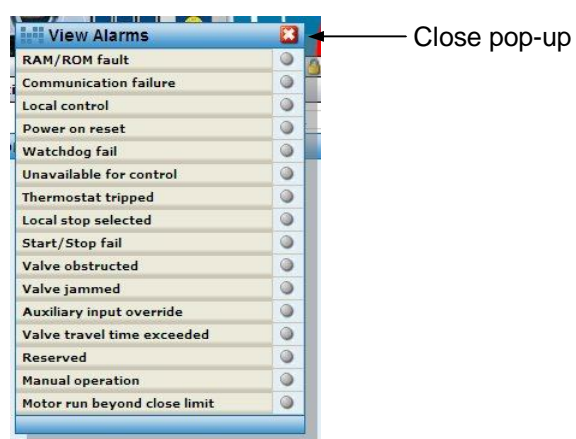
Fig 51:   *Wired IQ / IQT Alarms pop-up*

Pop-up screen shows the alarms on the actuator as red lights; grey is no alarm. Additional information on the meaning of these alarms is contained in the individual field unit manuals.

Torque Profile (2-wire loop and Wireless Field unit) - Available to all user levels

Fig 52:   *Wired and Wireless IQ / IQT Torque Profile pop-up*

Pop-up screen shows the last complete stroke torque profile generated by the actuator.

Event Log (2-wire loop Field unit) - Available to all user levels

Fig 53:   Wired IQ / IQT FCU Event Log pop-up

Pop-up screen showing a log of the last occasion on which the various control and alarm events occurred. For commands, the source of the command is also given.

Remote selected - local / remote selector in remote position.
Moving   - actuator centre column moving.
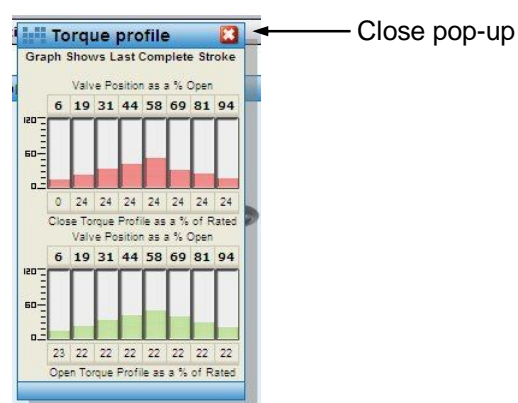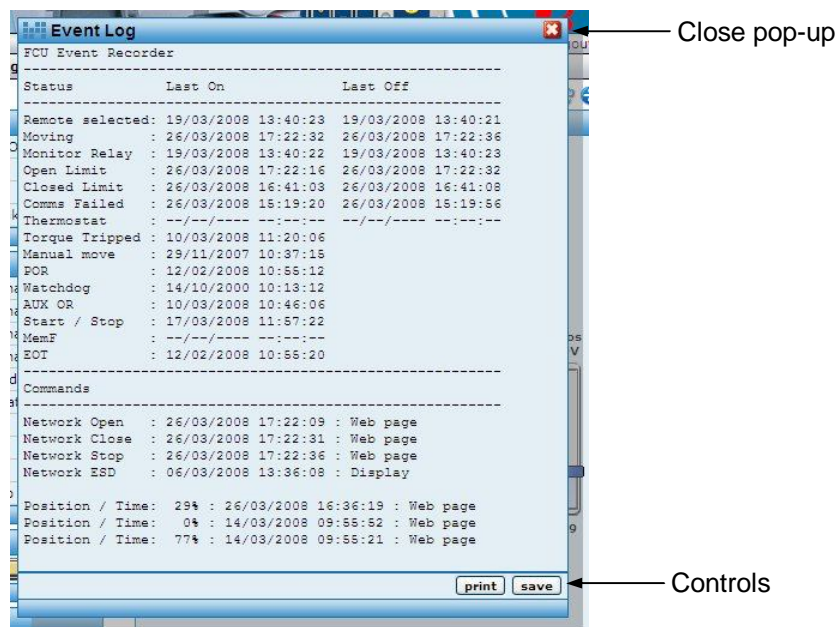Monitor Relay   - monitor relay alarm.
Open Limit   - open position limit switch.
Closed Limit   - closed position limit switch.
Comms Failed   - loss of network communication.
Thermostat   - motor thermostat tripped.
Torque Tripped   - torque limit level exceeded.
Manual move   - actuator moved by the handwheel.
POR   - power on reset.
Watchdog   - field unit watchdog alarm.
AUX OR   - auxiliary input present.
Start / Stop   - failure to respond to a remote control input.
MemF   - FCU memory chip RAM or ROM fault.
EOT   - motor running at end of travel.
Network Open   - open instruction over the control network.
Network Close   - close instruction over the control network.
Network Stop   - stop instruction over the control network.
Network ESD   - ESD instruction over the control network.
Position / Time   - last position control event.
Position / Time   - last but one position control event.
Position / Time   - last but two position control event.

Controls

Print   : Prints the logger data to a printer attached to the computer.
Save   : Saves the logger data to a file on the computer.

Parameters (Wireless Field unit) - Available to all user levels

Fig 54:   *Wireless IQ / IQT Parameters pop-up*

Pop-up screen shows the settings for all the parameters relating to the IQ / IQT actuator field unit. For users with Administrator level rights, the values can be edited. The parameters are used to determine the way in which the actuator responds to commands and reports data. Information on how to set these fields is contained in the actuator field unit manuals.

Controls

Save Settings   : Edited fields may be saved to the FCU; accessible by **Administrator** level users only.

Show Alarms (Wireless Field unit) - Available to all user levels

View Alarms	
EEPROM Checksum error	◯
Thermostat tripped	◯
Valve obstructed	◯
Valve jammed	◯
Local control	◯
Local stop selected	◯
Manual move	◯
End of travel movement	◯
Actuator stalled	◯
Monitor Relay	◯
Watchdog fail	◯
Battery low	◯
Battery flat	◯
General alarm	◯
Valve alarm	◯
Actuator alarm	◯
Network Card Fault	◯
Partial Stroke error	◯
Control Contention	◯
Mains Fault	◯
Comms Loss	◯
Loss of Phase	◯
24VDC fault	◯
Control alarm	◯
Position sensor fault	◯
Torque sensor fault	◯
Torque Tripped mid travel	◯
Local signal held	◯
ESD Active	◯
0x00 0x00 0x00 0x00 0x00 0x00 0x00	

Close pop-up

Fig 55:   Wireless IQ / IQT Alarms pop-up

Pop-up screen shows the alarms on the actuator as red lights; grey is no alarm. Additional information on the meaning of these alarms is contained in the individual field unit manuals.
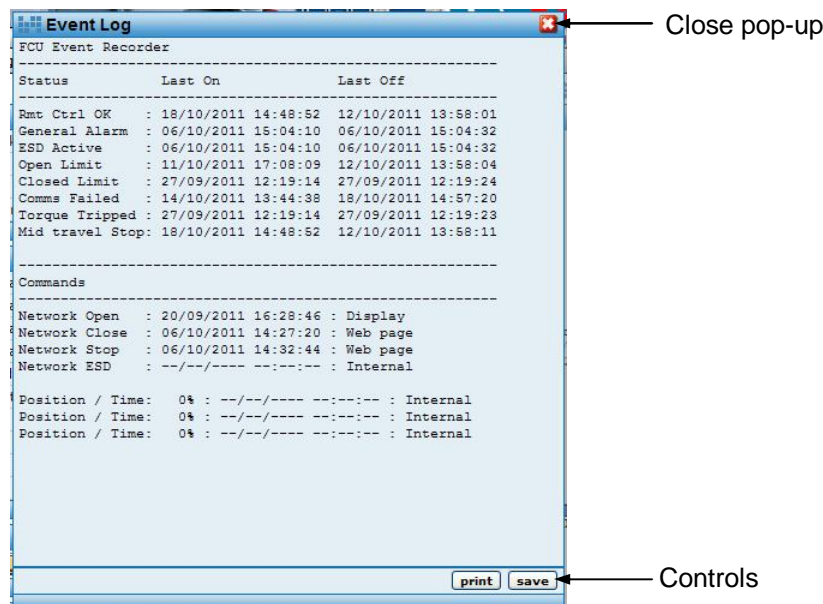
Event Log (Wireless Field unit) - Available to all user levels

Fig 56:   Wireless IQ / IQT FCU Event Log pop-up

Pop-up screen showing a log of the last occasion on which the various control and alarm events occurred. For commands, the source of the command is also given.

Rmt control OK - On means that the local / remote selector in remote position.
General Alarm   - Any Alarm present on the actuator e.g. Stall.
ESD Active   - ESD signal active on the actuator.
Open Limit   - open position limit switch.
Closed Limit   - closed position limit switch.
Comms Failed   - loss of network communication.
Torque Tripped - torque limit level exceeded.
Mid travel stop - motor stopped between open and close limits.
Network Open   - open instruction over the control network.
Network Close   - close instruction over the control network.
Network Stop   - stop instruction over the control network.
Network ESD   - ESD instruction over the control network.
Position / Time - last position control event.
Position / Time - last but one position control event.
Position / Time - last but two position control event.

Controls
Print   : Prints the logger data to a printer attached to the computer.
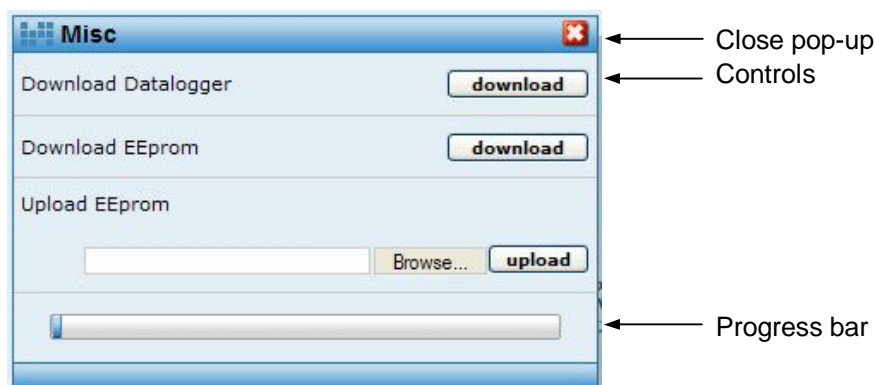Save   : Saves the logger data to a file on the computer.

Misc (Wireless Field unit) – Downloads available to all user levels, Upload only available to Admin user level

Fig 57:   *Wireless IQ / IQT Downloads pop-up*
Pop-up screen with controls to extract the Actuator Datalogger and Actuator Configuration files. It is also possible to load a configuration file to an actuator using this facility, assuming Admin login. The files that this facility creates are for viewing with the Rotork In-sight software, available on the Rotork web site.

Neighbour Table (Wireless Field unit) - Available to all user levels

Fig 58:   *Wireless Neighbour tables pop-up*
Pop-up screen that shows, for the field unit selected, the wireless neighbours that it has. It indicates the address of that neighbour and the Link Quality Index (LQI) of the signal from the device to its neighbour. The LQI is represented as a percentage value and is a good indication of signal quality and strength. A good signal would be in the range 93% to 100%. A reasonable signal would be in the range 61% to 92%; reasonable means that if environmental conditions deteriorate there is a greater potential for message retries and message failure.

It should be noted that rain, humidity and fog have a negligible effect on the wireless network. The greatest effect can be seen for heavy snow. By this, we mean snow that has settled on and around the antenna, i.e. 2 inches of snow packed around the antenna can cause a loss of about 10dBs.

Actuator Controls - Available to Write and Administrator user levels only

Open	: Command to open the valve fully.
Stop	: Command to stop the actuator in its present position.
Close	: Command to close the valve fully.
ESD	: Command to put the valve in its Emergency Shut Down position. (This can be 'stayput' or move to either the open or closed position).
Pos DV	: A slider control that is used to generate a setpoint position (Desired Value) for the valve in the range 0 - 100%.

All the controls have a confirmation pop-up, so that the action has to be confirmed before it takes place. Web page control must be enabled for these controls to work.

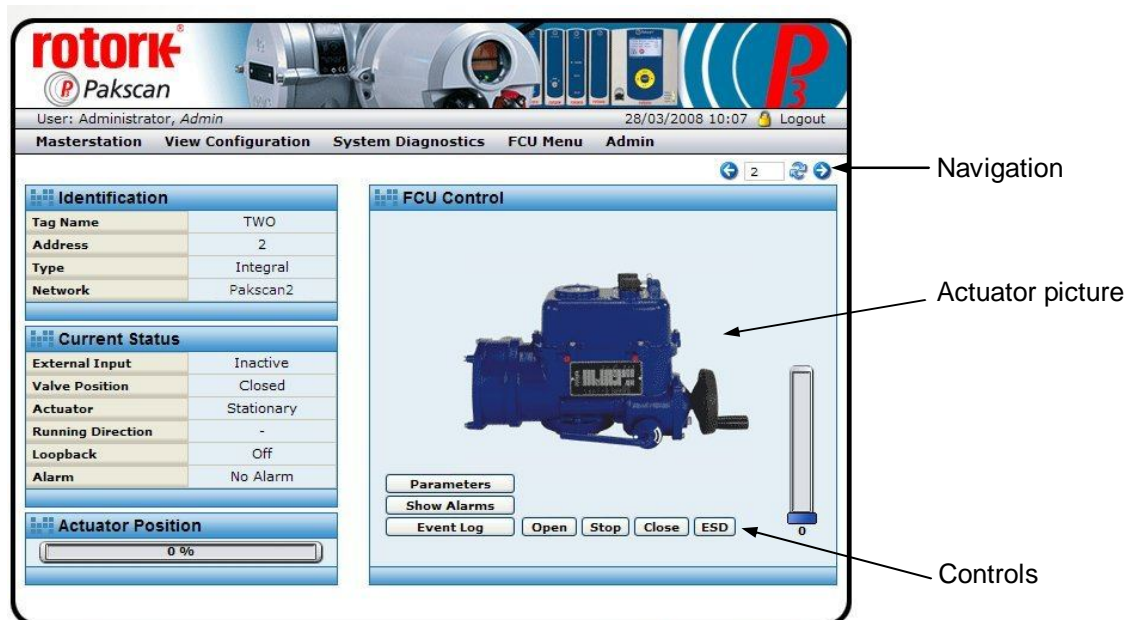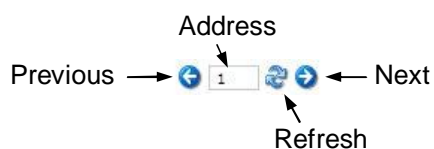### 7.5.13   FCU Control - Integral Actuator (2-wire loop only)

Fig 59:   Q actuator FCU Control Web page

This screen is accessible to Read, Write and Administrator user levels.

The Integral actuator FCU Control screen shows a control and status page for a Q type actuator. The screen has information relating to the device, its current condition and system parameters. Control of the actuator is permitted via the control buttons for users with write level access or higher. When not in communication, the screen may still be visited, but the picture has a large red cross over it to show a lack of communication.

Navigation

Navigation between the field units is either by returning to the previous screen, or by using the navigation buttons on this screen. Entering an address directly in the 'Address' box and clicking Refresh moves directly to the selected field unit.

Identification

Tag name	:	Identification tag given for this device.
Address	:	Network address.
Type	:	Shows the identified actuator type as Q.
Network	:	The network to which this device is connected (Pakscan 2 for 2-wire loop).

Current Status

The real time status of the actuator is listed in this pane on the screen:

External Input : Active or Inactive, shows the status of the input.

Valve Position : Current position, Closed, Open or Stopped Mid-Position.

Actuator : Moving or Stationary.

Running Direction : Opening or Closing.

Loopback : Off or On.

Alarm Status : No Alarm or Alarm.

Actuator Position

For actuators fitted with position feedback facilities, a bar graph shows the current actuator analogue position between 0 (closed) and 100% (open).

FCU Control web page Controls

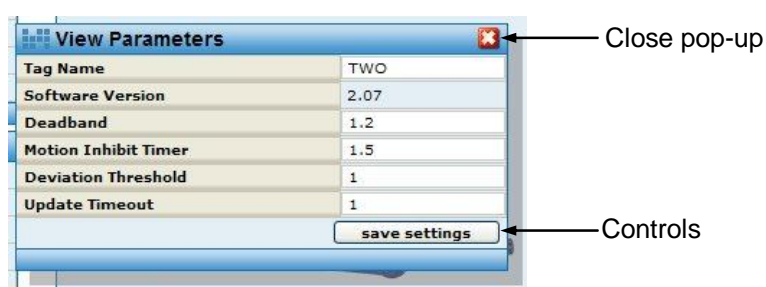**Parameters - Available to all user levels**

Fig 60:   Q Parameters pop-up

Pop-up screen shows the settings for all the parameters relating to the integral field unit. For users with Administrator level rights the values can be edited.

Controls

Save Settings : Edited fields may be saved to the FCU, accessible by **Administrator** level users only
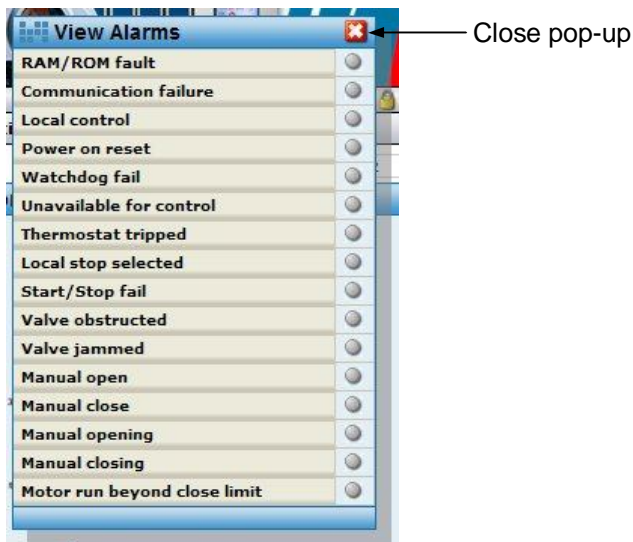
Show Alarms - Available by all user levels

Fig 61: *Q Alarms pop-up*

Pop-up screen shows the alarms on the actuator as red lights, grey is no alarm. Additional information on the meaning of these alarms is contained in the individual field unit manuals.
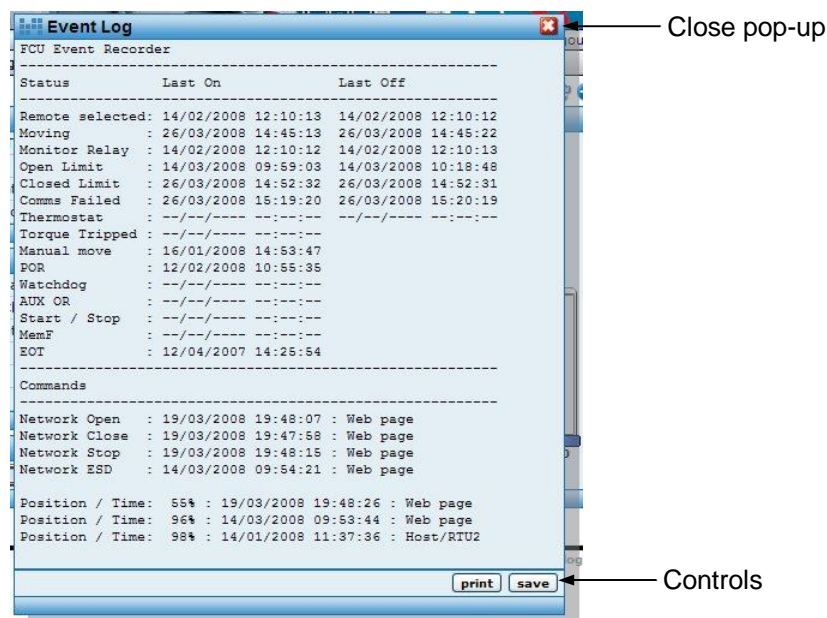
Event Log - Available to all user levels

Fig 62: *Q FCU Event Log pop-up*

Pop-up screen showing a log of the last occasion on which the various control and alarm events occurred. For commands, the source of the command is also given.

Remote selected - local remote selector in remote position.
Moving   - actuator centre column moving.
Monitor Relay   - monitor relay alarm.
Open Limit   - open position limit switch.
Closed Limit   - closed position limit switch.
Comms Failed   - loss of network communication.
Thermostat   - motor thermostat tripped.
Torque Tripped - torque limit level exceeded.
Manual move   - actuator moved by the handwheel.
POR   - power on reset.
Watchdog   - field unit watchdog alarm.
AUX OR   - auxiliary input present.
Start / Stop   - failure to respond to a remote control input.
MemF   - FCU memory chip fault.
EOT   - motor running at end of travel.
Network Open   - open instruction over the control network.
Network Close - close instruction over the control network.
Network Stop   - stop instruction over the control network.
Network ESD   - ESD instruction over the control network.
Position / Time - last position control event.
Position / Time - last but one position control event.
Position / Time - last but two position control event.

Controls

Print   : Prints the logger data to a printer attached to the computer.

Save   : Saves the logger data to a file on the computer.

Actuator Controls - Available to Write and Administrator user levels only

Open   : Command to open the valve fully.

Stop   : Command to stop the actuator in its present position.

Close   : Command to close the valve fully.

ESD   : Command to put the valve in its Emergency Shut Down position. (This can be 'stayput' or move to either the open or closed position).

Pos DV   : A slider control that is used to generate a setpoint position (Desired Value) for the valve in the range 0 - 100%.

All the controls have a confirmation pop-up, so that the action has to be confirmed before it takes place. Web page control must be enabled for these controls to work.

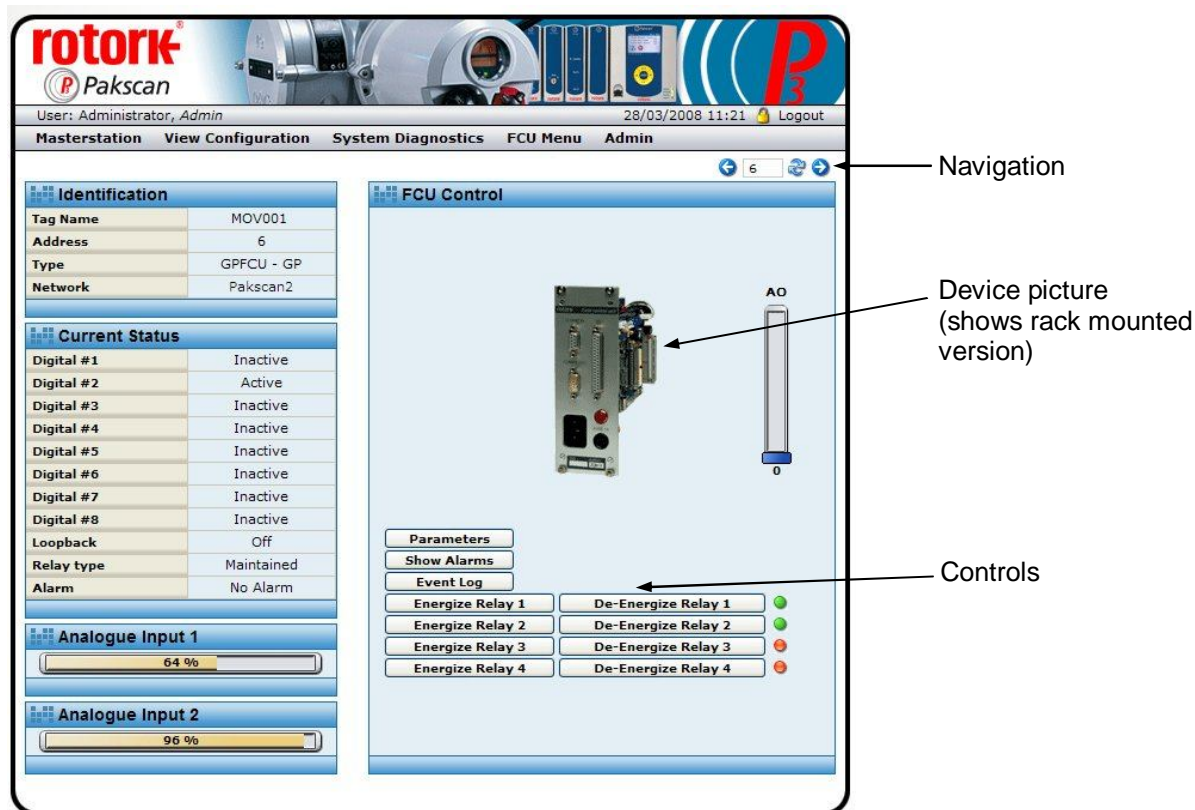### 7.5.14   FCU Control - General Purpose Field Control Unit (2-wire loop only)

Navigation

Device picture (shows rack mounted version)

Controls

Fig 63:   GPFCU Control web page

This screen is accessible to Read, Write and Administrator user levels.

The GPFCU Control screen shows a control and status page for a general purpose field control unit. The screen has information relating to the device, its current condition and system parameters. Control of the outputs is permitted via the control buttons for users with write level access or higher. When not in communication, the screen may still be visited, but the picture has a large red cross over it to show that a problem exists.

Navigation
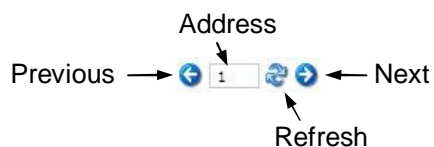
Navigation between the field units is either by returning to the previous screen, or by using the navigation buttons on this screen. Entering an address directly in the 'Address' box and clicking Refresh moves directly to the selected field unit.

Identification

    Tag name   : Identification tag given for this device.

    Address   : Network address.

    Type   : Shows the identified device type as GPFCU - GP.

    Network   : The network to which this device is connected (Pakscan 2 for 2-wire loop).

Current Status

    The real time status of the actuator is listed in this pane on the screen.

    Digital # 1 to # 8 : Digital input signal status, Active or Inactive.

    Loopback   : Off or On.

    Relay Type   : Fleeting or Maintained outputs from the relays.

    Alarm Status   : No Alarm or Alarm.

Analogue Input 1 and 2

    For the two analogue input channels a bar graph shows the current analogue input value between 0 (closed) and 100% (open).

FCU Control web page Controls

Parameters - Available to all user levels

Fig 64:   *GPFCU Parameters pop-up*

    Pop-up screen shows the settings for all the parameters relating to the general purpose field control unit. For users with Administrator level rights, the values can be edited.

    Controls

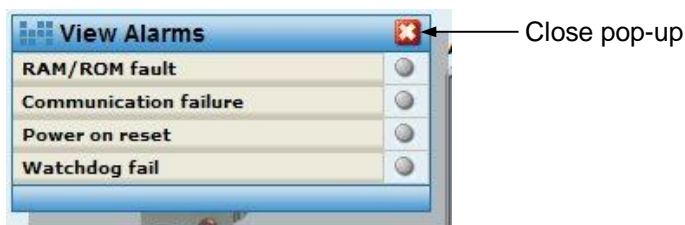   Save Settings   : Edited fields may be saved, accessible by **Administrator** level users only.

Show Alarms - Available to all user levels

Close pop-up

Fig 65: GPFCU Alarms pop-up

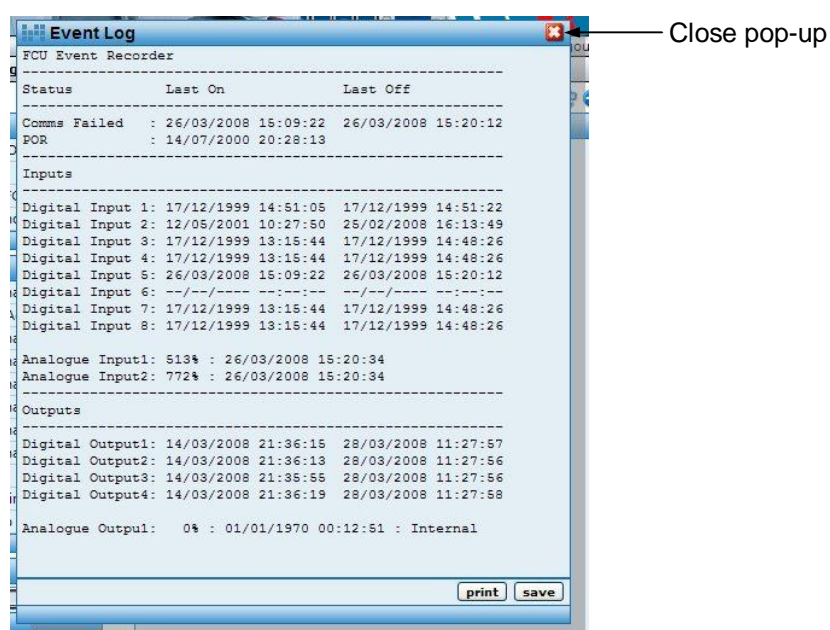Pop-up screen shows the alarms on the actuator as red lights; grey is no alarm.

Event Log - Available to all user levels

Close pop-up

Fig 66: GPFCU Event Log pop-up

Pop-up screen showing a log of the last occasion on which the various alarms, input and output events occurred. For commands, the source of the command is also given.

Comms Failed	- loss of communication with the field unit.
POR	- power on reset.
Digital Input 1-8	- when turned on and off.
Analogue I/P 1-2	- when last updated.
Digital Output 1-4	- when energised and de-energised.
Analogue Output	- when last altered and by which source.

Controls

Print	:	Prints the logger data to a printer attached to the computer.
Save	:	Saves the logger data to a file on the computer.

GPFCU Controls - Available to Write and Administrator user levels only

Energise : Command to energise the relays (green light when energised).
Relay 1-4

De-energise : Command to de-energise the relays (red light when de-energised).
Relay 1-4

AO : A slider control that is used to generate a 0-5volt analogue output. Slider range 0 - 100%.

All the controls have a confirmation pop-up, so that the action has to be confirmed before it takes place.

7.5.15 Admin

Fig 67: Administrator Level

This screen is only accessible to Administrator user levels.

When logged in at Administrator level, the top of the screen menu list includes the Admin button. Clicking on this button gives entry to the Administrator level screens.
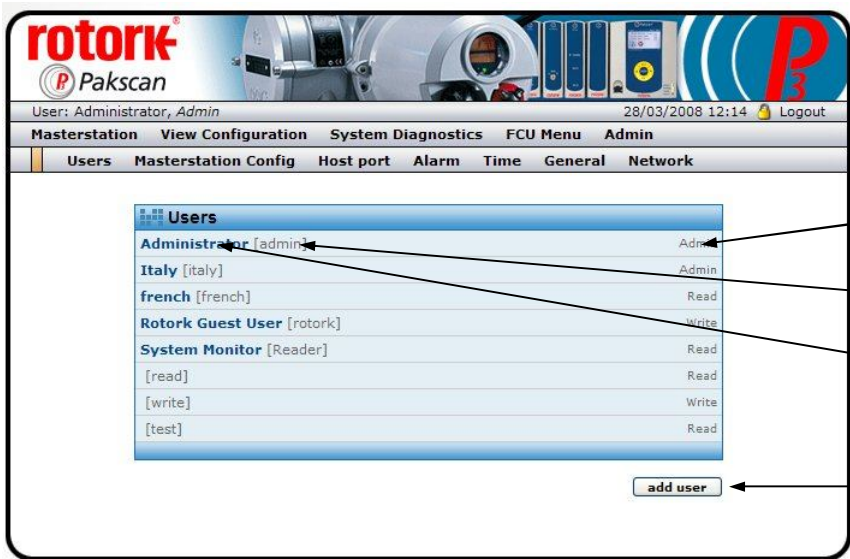
Admin button

7.5.16 Users

User Level

User ID

Name

Controls

Fig 68: Users web page

This screen is only accessible to Administrator user level.

The 'Users' screen shows all the users currently entered into the system. The actual user at any time is shown on the top left of the menu bar.

Each user has a Name, a User ID, a User Level and a Password. When logging in to the system, to gain entry, the User ID and Password are required. The screen shows the Name, User ID and User Level; the password is not shown and cannot be revealed on any of the screens.

Every system includes a default User ID of 'admin' and Password of 'admin' on delivery, in order that the system can be set up and commissioned. The user ID 'admin' cannot be removed, but the Password should be changed as soon as possible to protect the system against unauthorised access.

Name	Name of the current user, displayed on the top bar.

User ID	Identification used to gain entry to the system, shown in user list.
Password	Secret code of letters (and numbers) used to gain entry to the system. Not shown on the system.
User Level	Indication of access level permitted for this user, shown on the top bar.

Controls - Available to Administrators only

Add user   : Click this button to bring up the screen to add a user.
Username   : Click on a user name (e.g. Administrator) to bring up the Modify User
                      screen for editing user details.

Fig 69:   Add User web page

The Add User screen contains the fields to be completed for each permitted user, either by completing the data box, selecting from a drop-down box or selecting a radio button.

User ID   : Enter a unique name to use when logging in to the system.
Name   : Enter a name to be used in all emails and on the system logs.
                   Several users can have the same name, but this is not recommended.
Email   : If Email messages concerning the system alarms are to be sent to this
                   user, enter a valid Email address.
Mobile   : If text messages are to be sent to a mobile phone associated with this
                   user, enter the complete phone number here.
Alarm User   : Select 'Yes' or 'No' for the choice of sending Emails and Text messages to
                   this user.
Email Master   : Select 'Yes' or 'No' for the choice of sending the master station log file via

station Log		Email.
Language	:	Select the language to be used on the screens. Choices are English, Spanish, French, German and Italian.
User Level	:	Select between Read, Write and Admin levels.
Password	:	Enter a unique password of letters and/or numbers kept secret by this user.
Repeat Password	:	Enter the same password as above.
Back	:	Exit the screen without saving anything and return to the previous screen.
Save Settings	:	Save the details of this user (either new or edited values).

Fig 70:   Modify User web page

The Modify User screen allows user details to be altered or a user to be removed. A User cannot delete himself from the system. So, here in the example, the User ID of 'admin' is greyed out, since this is the actual user.

Remove	:	Delete this entry on the system. A User cannot delete themselves, only those with less access rights. If the User selects his own entry to modify the button is greyed out.

7.5.17   Master station Configuration

The master station configuration page is used to set the parameters required for successful operation of the system and the parameters for the option modules fitted. In addition, it may be used to enter the site name and tag name of the system and various security settings. The values set in these parameters can be viewed under the 'View Configuration' button, but they may only be altered by users logged in at Administrator level.

The Master station settings relate to the overall performance of the system and common features and actions, irrespective of the option module fitted. Where these settings are relevant, they apply to all the option modules in the master station.

The Option module settings relate to the particular option module fitted in the Option 1 and Option 2 slots.

Fig 71:   Master station configuration web page: General Settings

This screen is only accessible to Administrator user level.

Masterstation Configuration [General Settings]

Site Name   : A text field in which a description of the site can be entered for identification purposes.

Tag Name   : A text field in which a tag identifier for this particular master station on the site can be entered.

Option 1 and Option 2 Modbus Address : A numeric field for the address number. When addressing the P3 master station using a host, the user must use the appropriate Modbus address. It is possible to fit up to 2 network option modules to the P3 master station. Each option module will have its own Modbus address, therefore there are up to 2 Modbus addresses to set up, one for each option module fitted. In a system with only 1 option module fitted, only the address for the appropriate option module fitted is required to be set up.

The default value is **240** for a Pakscan 2 Loop option module and **200** for a Pakscan wireless option module. It is recommended that his is changed to avoid conflict with any new system added

Note for Pakscan 2 Loop module Modbus Addressing

In some cases when using Pakscan Generic Modbus protocol settings, the master station will respond to more than one address; and the setting here is the Base address. There is more information on the base address and offset addresses in the Pakscan Modbus Protocol document (PUB059-003 formerly S171E).

Monitoring wireless and Control wired : Only in a system where each actuator has a wired and a wireless Pakscan module fitted, should this be enabled. This feature will pair up the wired and wireless modules and enable them to be shown together in the FCU menu web page. The pairings will be:

- **the first wired address with the first wireless address,**
- **the second wired address with the second wireless address,**
- **...... and so on.**

Therefore in a system where the wireless addresses start at 61 (wired always start from 1) the pairings would be:

- Wired address 1 with wireless address 61
- Wired address 2 with wireless address 62
- Wired address 3 with wireless address 63
- ..... and so on.

The FCU menu will appear as below:

FCU Menu						
Address	**Tag Name**	**Type**	**Network**	**Alarm**	**Comms Fail**	**Navigation**
1	-	IQT	Pakscan2	●	●	fcu control
61	-	IQT	Wireless	○	○	fcu monitoring
2	-	IQ	Pakscan2	●	●	fcu control
62	-	IQ	Wireless	○	○	fcu monitoring

Hot Standby   : Either 'Enabled' or 'Disabled'. When there is a partner module acting as

Module		a standby unit this option should be set to 'Enabled' to allow exchange of data between the two modules.
ESD Settings	:	These five drop-down boxes can each be set to 'Enable' or 'Disable' the related Emergency Shut Down signal, depending on the particular site requirements. In general the settings should be 'Disabled' unless the particular Emergency Shut Down function is required. The action for each individual actuator has to be set locally on the actuator to either close, open or stay put (no movement on receipt of the ESD signal), as required for each valve; refer to individual actuator manuals.
Command Settings	:	These five drop-down boxes can each be set to 'Enable' or 'Disable' the host system commands to the actuators and field units from the indicated source of the signal. For example, commands over the Ethernet connection can be disabled, whilst those from Serial Port 1 can be enabled. Ethernet commands are those sent via the Ethernet ports from the host system using Modbus TCP. Commands on the individual field unit web pages can also be disabled. Serial Port 1 and Serial Port 2 are the RS-232/RS-485 Modbus RTU ports, which are commonly used for control and monitoring. The Keypad is the control source on the front panel of the CPU module.
Copy Options	:	These four drop-down boxes can each be set to 'Enable' or 'Disable' the copying of information between the A side and B side CPU and Option modules in a hot standby system. They do not appear in a single module system.

Settings	-	Enable to copy *all* the settings, except those listed below, between the units.
Address	-	Enable to copy the Modbus addresses of the CPU (P3 option) and Pakscan Loop option module between the units.
Tag	-	Enable to copy the Site name and system Tag name between the units.
IP	-	Enable to copy the IP address and Ethernet settings between the units

Display Language	:	This drop-down box contains the options enabling the system language to be chosen. The options are English, Spanish (Espanol), French (Francais), German (Deutsch) and Italian (Italiano).
Security Settings	:	A text box is provided in which the system PIN can be entered, and a drop-down box provides the options for access permission when using the CPU keypad and screen.

Note that the 'Command Settings' above can be used to prevent keypad commands under all circumstances, but when the keypad is enabled the security settings below will apply.

PIN - The Password number is a variable between 0 and 9999. When a number is entered, it indicates that the PIN must be used for settings or commands to be allowed from the CPU keypad in accordance with the associated drop-down box setting.

Security - The drop-down box contains the options for selecting the

protection afforded against inappropriate actions when using   the CPU keypad.

None : All settings and control commands accessible via the keypad without protection by a PIN.

Set up: Control commands accessible via the keypad without a PIN, but all setting changes via the keypad require the PIN to be entered first.

Set up and Control: Any control command action or setting changes via the keypad require the PIN to be entered.

Locked : No keypad access permitted for any control commands or setting changes whilst there is host activity on any of the serial or Ethernet data links. [If all serial and Ethernet communication links are inactive for 5 seconds then keypad commands can be entered provided the PIN is entered (as with the Set up and Control level)].

Software Version	:	The version of software fitted to the CPU module. In hot standby systems the modules in both the A and B side should have the same version of software.
Country Code	:	This setting relates to the wireless option only. Whilst the frequency band over which the wireless communicates is a globally available band, there are frequencies within this band that certain countries do not allow. This parameter is set up during the first 5 times that the master station is powered up or by using the HMI menu A3F. This setting will ensure that that the channels made available for selection within the wireless option module are only those legally available within that particular country.
Number of Channels	:	This value is derived from the actual hardware of the CPU and indicates the maximum number of actuators or field units that can be connected to this system. The field units can be split between the option modules fitted.
FCU distribution between Option Slots	:	Using the slider bar the user is able to select the number of field units connected to each option module fitted in batches of 60. Simply select and drag the bar to the appropriate setting with the mouse, the text above the bar will indicate what has been selected.

The bar will only allow selection up to the maximum number of field units available on the master station in question.

This bar only selects the **number of field units** allocated to the two option slots and **not** the address range of the field units on the option slot network. The Pakscan 2 loop actuators will always start at address 1. In the example shown on the next page, where there are 180 devices on the Pakscan 2 loop module, the addresses 1 to 180 will be for the Pakscan 2 loop units. The starting address for the wireless devices is set up in the wireless configuration section and this would logically (but not necessarily) be set to 181. This would mean that the addresses for the 60 wireless devices can range between 181 and 240.
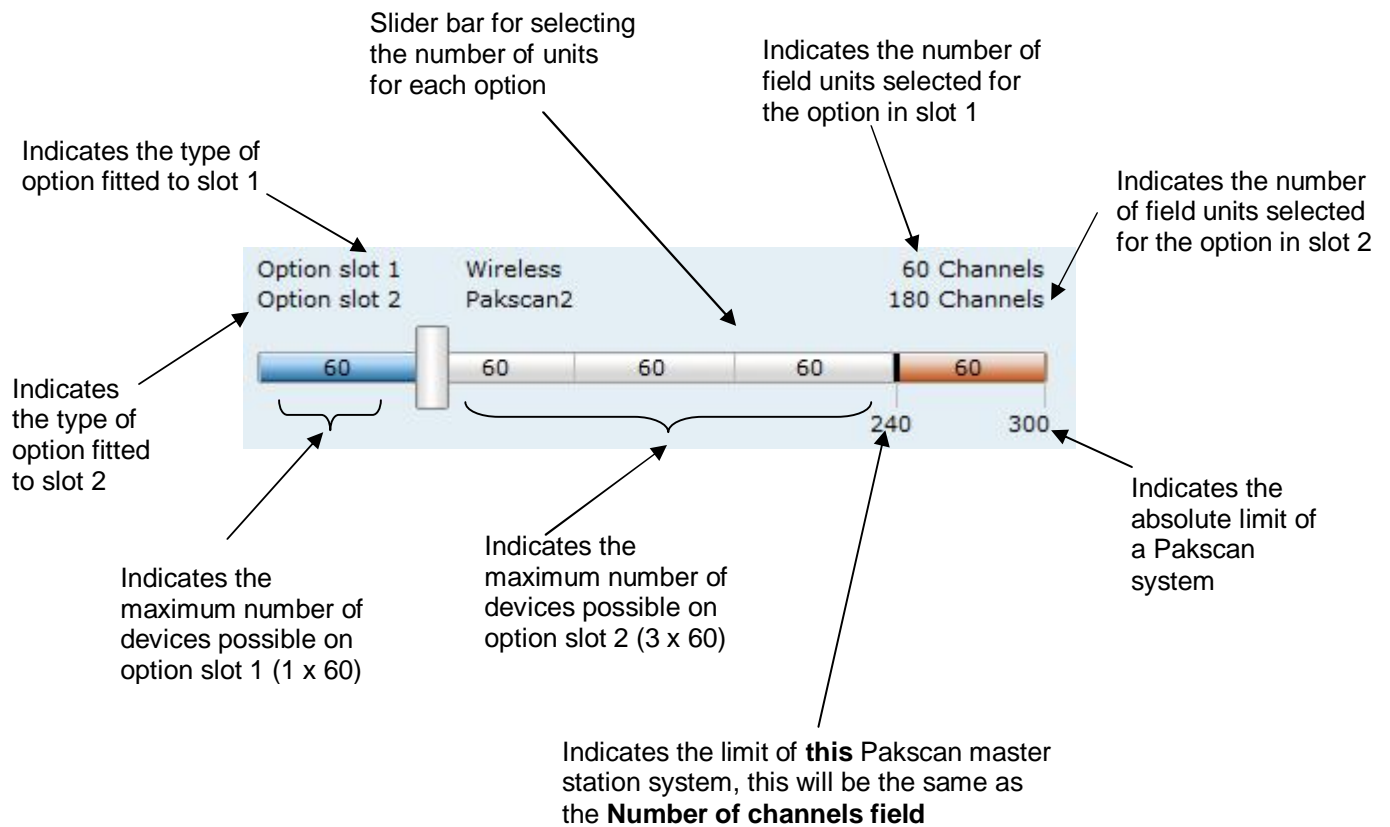
Slider bar for selecting
the number of units
for each option

Indicates the number of
field units selected for
the option in slot 1

Indicates the type of
option fitted to slot 1

Indicates the number
of field units selected
for the option in slot 2

Option slot 1   Wireless   60 Channels
Option slot 2   Pakscan2   180 Channels

| 60 | 60 | 60 | 60 | 60 |

240   300

Indicates
the type of
option fitted
to slot 2

Indicates the absolute limit of
a Pakscan
system

Indicates the
maximum number of
devices possible on
option slot 1 (1 x 60)

Indicates the
maximum number of
devices possible on
option slot 2 (3 x 60)

Indicates the limit of **this** Pakscan master
station system, this will be the same as
the **Number of channels field**

Fig 72:   *Web page Field unit distribut*

Controls

     print page   : Prints the settings to a printer attached to the computer.
     save settings   : Saves the settings to the master station CPU module. Until they are saved
                            any alterations to the settings will not take effect.

Masterstation Configuration [Pakscan 2 Loop]

The Pakscan 2 Loop option module controls the actuators and field units over a 2-wire cable wired in a ring or loop, visiting each actuator in turn. The data signal is a modulated 20 mA current and the system includes automatic cable failure protection and detection.

Fig 73:   Master station configuration web page: Pakscan 2 Loop

Software Version : The version of software fitted to the Pakscan 2 Loop option module. In hot standby systems the modules on both the A and B side should have the same version of software.

Highest FCU   : This text box contains the setting for the highest address used for an actuator (or field unit) on the 2-wire loop. The Pakscan 2 Loop module polls all field units from address 1 up to this highest address. The loop scan time is minimised by restricting the polling to only those field units that should be present and scanning up to the highest address. All the addresses in the selected range should be used and gaps in the address range should be avoided. Gaps or unused addresses cause the system to run more slowly as the unused addresses are still checked. In addition, unused addresses will generate a communication failure alarm.

Loop Speed   : This shows the current loop scanning speed (loop baud rate) and the drop-down box allows a desired loop speed to be selected. The choices are 2400, 1200, 600, 300 and 110 baud. When a new speed is entered it will take effect as soon as the values are saved. The setting applies to the Pakscan 2 Loop option module only and the actuators must be changed individually.

New Loop Speed: The drop-down box allows a new scanning speed (loop baud rate) to be selected for the field units in the actuators. The new speed will be adopted next time the loop is reconfigured. A change here should be mirrored by a change in the loop speed setting above. It is possible to select rates in the range one step up or two steps down from the current speed.

If the loop communication is not stable, it is often necessary to reduce the speed to improve reliability. If the field units are all in communication with the master station, this facility to globally change the speed of all the field units can be used to assist in improving the reliability.

Loop Speed Doubling : On a stable loop it is possible to halve the loop scan time by doubling the data speed using this setting. Care is needed to ensure that the loop continues to be stable, since the use of this feature slightly reduces the system's capability to reject interference from pumps and motors.

Retain Data on Loss of Communication : Normally the database information about an actuator is cleared to zeros if communication with the actuator is lost. This ensures that the false valve position information is not transmitted to the host system during the loss of communication. A single 'Comms Fail' data bit is set. This system setting allows the data to be kept at the last value received from the actuator. Note that the data is retained indefinitely and does not necessarily reflect the true actuator status.

DV Convert : This option can be used to ensure that 100% and 0% Desired Value outputs to the IQ, IQT, Skil and EH actuators are transformed into actions to make the actuator run to the fully open (100%) and fully closed (0%) positions. The message is converted from a DV command to an Open or Close command. This is useful for positioning actuators, where it is possible that the valve will not fully shut or open when moved by only a small amount. When used for tight shut-off valves, with analogue position control only, the setting should be ON; the default is OFF.

If limited range positioning is selected, only enable DV Convert if you wish the valve to travel to the fully open and fully closed positions.

Host Port 1 Database Selection : The drop-down box allows the database organisation use on this port to be selected. The choices are Generic Modbus, Honeywell EPLCG Modbus, Yokogawa Modbus and Honeywell SI Modbus.

Host Port 2 Database Selection : The drop-down box allows the database organisation used on this port to be selected. The choices are the same as for Host Port 1.

Ethernet Database Selection : The drop-down box allows the database organisation use on the Ethernet ports to be selected. The choices are the same as for Host Port 1.

Port Alarms : This drop-down box allows port alarm handling to be configured. Alarms can either operate completely independently ('separate') for each port, or can be linked such that the same alarm information is always reported, regardless of which port is used.

Alarms must be read and accepted before they can clear and return to normal. If configured as separate, alarm reading and acceptance must be done separately for each of the three ports. This ensures that the different hosts see all the alarms. When the alarms are linked, accepting an alarm on one port accepts the alarm on all the other ports as well.

The status screen displays for alarm indication cannot be linked to the serial communications alarm handling.

Linking the port alarm operations is useful in dual redundant serial link configurations between the master station and the host computer.

Controls

Save Settings : Saves the settings to the Pakscan 2 Loop option module. Until they are saved, any alterations to the settings will not take effect.

To print out the settings use the Print Page button below the Master station Configuration section of the screen.

Masterstation Configuration [Pakscan 3 Wireless]

The Pakscan 3 Wireless option module controls the actuators and field units over a wireless network.

Fig 74:   Master station configuration web page: Pakscan 3 Wireless

Software version	:	The version of software fitted to the Pakscan 3 option module. In hot standby systems the modules on both the A and B side should have the same version of software.
Coordinator Software version	:	The version of software fitted to the Pakscan 3 option module, relating to the radio functions. In hot standby systems the modules on both the A and B side should have the same version of software.
Lowest FCU address on this card	:	This field indicates the starting address of the field units connected to this option module. It is important to ensure that there is no overlap of addresses between option modules. Where the wireless module is the only module fitted the address can be '1'. If a wired option network module is fitted, the wireless address should be a value above the wired network limit. For example, where there are 180 wired devices and 60 wireless devices (as shown in Fig 66), the lowest wireless address would be set to 181.

Total FCU's expected on this option card	:	The total number of field units that are expected to be found on this network associated with this module. The master station will expect to find this number of field units on the network starting at the address set.
Total Wireless Repeaters expected on this option card	:	The total number of wireless Repeaters that are expected to be found on the network associated with this module. There can be a maximum of 15 repeaters fitted to a wireless network.
Wireless Network PAN ID	:	The PAN ID is the Personal Area Network Identification number of the network attached to this option module. For a device to connect to the master station it must have a PAN ID the same as the master station. The default value is DA 15 and the range is 00 00 to Hex FF FF. Where there are multiple networks in close proximity, the PAN IDs should be set to unique numbers.
Retain Data on Loss of Communication	:	Normally the database information about an actuator is cleared to zeros if communication with the actuator is lost. This ensures that the false valve position information is not transmitted to the host system during the loss of communication. A single 'Comms Fail' data bit is set. This system setting allows the data to be kept at the last value received from the actuator. Note that the data is retained indefinitely and does not necessarily reflect the true actuator status.
AES Key	:	Pakscan wireless employs the Advanced Encryption Standard (AES) as a method of protecting the command messages to devices on the network. The AES key must be the same on all devices on the network and the master station. To protect the commands the AES key should be kept secret. The AES key is a 128bit hexadecimal value, if a device does not have the same AES key as the master station, it will not be able to be commanded by the master station.
RF Channel	:	The range of frequencies in the 2.4GHz band over which the Pakscan wireless network communicates is split into channels. Some countries will not accept communication over certain frequencies. Therefore, the country code chosen in the general settings will ensure that the channels available to be selected using this drop-down box are only those that are legal.
Third party devices fitted	:	Using a Wireless Modbus Adapter (WMA) it is possible to connect other manufacturers' devices into the Pakscan Wireless network. If 'yes' is selected in the drop-down box and the setting is saved, the web page will change to show the following:

The user may then select the Modbus address of the device or devices that are connected to the WMA, It is possible to have 47 Modbus devices integrated into the network using addresses 201 to 247. It is possible to have more than one Modbus device connected to a WMA. All Modbus devices must have unique addresses that must not clash

with other Modbus devices in the network. For Modbus devices fitted in the Pakscan wireless network, the master station system is effectively used as a transparent transport mechanism i.e. the host sends Modbus requests to the master station as though addressing the device directly.

Controls

Save Settings : Saves the settings to the Pakscan 2 Loop option module. Until they are saved, any alterations to the settings will not take effect.

To print out the settings use the Print Page button below the Master station Configuration section of the screen.

7.5.18   Host Port Configuration

Fig 75:   *Host Port Configuration web page*

This screen is only accessible to Administrator user level.

The host port configuration page allows the settings for the serial and Ethernet ports to be made. The two serial ports (ports 1 and 2) are independent from one another whilst the Ethernet ports (ports 3 and 4) are linked together.

Host Port 1

Baud Rate : This drop-down box allows the communication speed (baud rate) for the serial port to be selected. The choices are 115200; 57600; 38400; 19200; 9600; 4800 or 2400.

Parity : This box sets the message parity used by this port. The choices are None; Always 0; Odd or Even parity.

Standby Mode : The performance of the port when the CPU module is in standby mode is set by this drop-down box. The Serial Port should appear as Passive if the Cross Connect DIP switch on the system back plane is set to 'cross-connect'.
If the port is set to RS-485 highway and is being used on a multi-drop highway, it *must* be set to passive. If it is not shown correctly it probably means the DIP switch is incorrectly set.
When the port is set to 'Active' it will respond to incoming messages with a reply; when set to 'Passive' it will not reply. If the highway is multi-drop, then these replies will conflict with those from the CPU in Main mode.
Note that a CPU in main mode is active and always replies to incoming messages.

Cross Connected: Either Yes or No, indicating the status of the cross-connect DIP switch on the back plane. A system using RS-485 communication and a Hot Standby pair should be set to 'Cross-Connect' and display 'Yes'.

Physical Interface: Either RS-232 or RS-485, showing the switch setting for the physical interface from the CPU module.

Host Port 2

Baud Rate : This drop-down box allows the communication speed (baud rate) for the serial port to be selected. The choices are 115200; 57600; 38400; 19200; 9600; 4800 or 2400.

Parity : This box sets the message parity used by this port. The choices are None; Always 0; Odd or Even parity.

Standby Mode : The performance of the port when the CPU module is in standby mode is set by this drop-down box. The Serial Port should appear as Passive if the Cross Connect DIP switch on the system back plane is set to 'cross connect'.
If the port is set to RS-485 highway and is being used on a multi-drop highway, it *must* be set to passive. If it is not shown correctly, it probably means the DIP switch is incorrectly set.
When the port is set to 'Active' it will respond to incoming messages with a reply; when set to 'Passive' it will not reply. If the highway is multi-drop, then these replies will conflict with those from the CPU in Main mode.
Note that a CPU in main mode is active and always replies to incoming messages.

Cross-Connected: Either Yes or No, indicating the status of the cross connect DIP switch on the back plane. A system using RS-485 communication and a Hot Standby pair should be set to 'Cross-Connect' and display 'Yes'.

Physical Interface: Either RS-232 or RS-485, showing the switch setting for the physical interface from the CPU module.

Ethernet Port

Standby Mode : The performance of the port when the CPU module is in standby mode is set by this drop-down box. The Ethernet Port should be set as Passive if the system includes a hot standby CPU to avoid conflicts in communications.

When the port is set to 'Active' it will respond to incoming messages with a reply, when set to 'Passive' it will not reply.

Note that a CPU in main mode is active and always replies to incoming messages.

IP Authentication : The two IP addresses that can be set here are to do with system access permission. When controlling the system via Ethernet and Modbus TCP, it is possible to increase the system security and only permit access from specified IP locations. If both the values set here are 0.0.0.0 then any IP address can access the system.

When a specific IP address is entered in either IP Number 1 or IP Number 2, the system only allows access for modbus messages originating from those addresses. Note that all access, including Read only access, is restricted by the entries.

Controls

Save Settings : Saves the settings for the ports. Until they are saved any alterations to the settings will not take effect.

Modbus Message : Brings up the Modbus test screen where specific messages can be sent to the system via the web page.

Fig 76:   *Modbus Message Generator web page*

The Modbus Message screen allows a specific query to be sent to the system and the response to be viewed.

Modbus Message Query

Address	: The CPU master station Modbus address (in the range 0 -247).
Function Code	: Modbus function code to read or write register, discrete or coil.
Data	: Modbus data relating to the query message. There is no need to include the CRC in the data field as the system generates this automatically. There should be no spaces in the data field.

Controls

Send Query	: Transmits the message to the master station.

Modbus Message Response

Address	: The address of the responding system. It will match the query address.
Function Code	: Modbus function code to read or write register, discrete or coil.
Data	: Modbus data reply, without a CRC. There will be no spaces in the data field.

Example:
Read the number of field units connected to the system; generic database is set up. Refer to PUB059-003 (formerly S171E) for the mapping of the Modbus registers. Number of FCUs is at master station register 0007. Function code 03 (holding register read) can be used. The Modbus function would be:

Modbus Address	function code	register to start read	number of registers to read
01	03	00 07	00 01

The address and function code should be entered in the relevant spaces and the data field should contain the rest of the function, this field should be entered with no spaces. When the send query button is pressed the result will be shown.

Fig 77:   Modbus Message Example web page

Here the data shows that 2 bytes of data are present in the message (02) and the data is 00 19. The 19hex is the number of field units fitted to the A side of the loop.

7.5.19 Alarms

Fig 78: *Alarm Reporting Set up web page*

This screen is only accessible to Administrator user level.

This page is used to set up the email alarm reporting from the system to the dedicated recipients as specified in the user set up screen. Each system user may be specified to receive alarm messages as emails or by text when their log-in credentials are specified. Refer to the section on Users to see how this is set up. The Alarm page has two sections. The first deals with the way emails are to be generated and the specifying of a suitable SMTP server, whilst the second specifies which events will cause messages to be sent.

Alarm Email Settings

Email Alarm	:	Set to Enable or Disable the whole process.
SMTP Server	:	Specifies the server that the master station will use for forwarding emails. This is either a domain name or IP address for the server on which the email account has been set.
SMTP Authentication	:	If the domain server supports SMTP authentication, then set this to Enable and complete the Authentication parameters. (More information on SMTP Authentication can be found in RFC 4954 available on the internet.) Authentication Method - auto, plain, login or cram-md5; usually set to login. Username - the email user name for the master station or an identifier. Password - the chosen verification password for authentication of the messages from the master station to the server.
Sender	:	A name to identify the master station, it could be the tag name.
Reply Path	:	The email address of the master station or an alternative reply address for return messages.
Test Email :		Enter a valid email address to send a test message to in order to ensure the system is working correctly; then click on 'Test'.

Controls

Test	:	Sends a test email to the specified address.
Save Settings	:	Saves the 'Alarm Email' Settings.

FCU Alarm

This table lists the devices on the field network by address and tag number. The right hand side box, when clicked, toggles between a tick and no tick. A tick indicates that if any alarm occurs on this field unit, it will be reported by the email or text facility.

Controls

Clear All	:	Removes any ticks from all the boxes in the list.
Set All	:	Adds a tick in all the boxes in the list.
Save Settings	:	Saves the FCU Alarm list settings.

Event List

This table lists all the Master station and Option module alarms that can be used to initiate an alarm email or text. The list is split into two parts relating to the CPU module and the Option module(s).

Controls

Save Settings	:	Saves the Event List settings

7.5.20 Time

Fig 79:   Time Settings web page

> This screen is only accessible to Administrator user level.

The master station keeps track of time and date in order to correctly mark events in the logs and to timestamp the emails sent. The date can be in European or American format and the clock can be synchronised with a network time server when an Internet connection is provided.

Time Settings

Date	:	The date can be displayed as Day/Month/Year or Month/Day/Year by choosing from the drop-down box.
Time	:	Shows the current time. This can be altered by clicking in the box and entering the new time (hr, min, sec) as required. If NTP has been set up and enabled this will update automatically, otherwise the time can be checked periodically and corrected here.
Timezone	:	Select the desired time zone from the drop-down Controls entry requires that the master station reboots.
Network Time Protocol	: :	NTP is a protocol designed to synchronize the clocks of computers over a network. If this feature is being used it needs to be 'Enabled' by selecting the correct setting here.
NTP Server	:	The time server selected is pool.ntp.org which selects from a pool of time server volunteers. Other NTP servers are available and can be used, in which case the entry here should be altered.
Update Interval	:	This drop-down box allows the interval between time checks with the server to be altered between 10 minutes and 2 hours.

Controls

Save Settings	:	Any changes are not implemented until the Save Settings button is clicked. Changes to these settings will require a reboot of the system. The web page will prompt this.

7.5.21   General
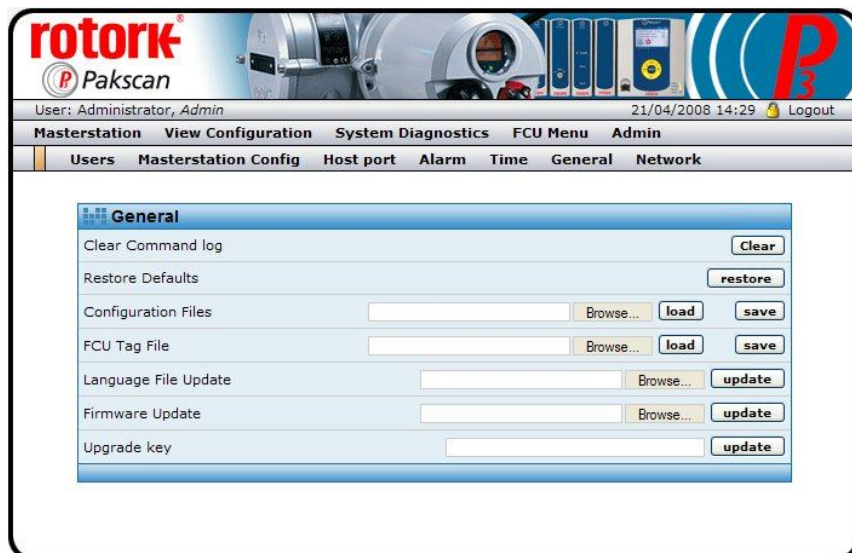
Fig 80:   General web page

This screen is only accessible to Administrator user level.

The General screen contains facilities for upgrading and maintaining the master station.

General

Clear Command Log	:	The master station data logger (which can be found under System Diagnostics, ms datalogger) creates a file for all the recorded events. The Clear Command button empties this file. If required, the file can be saved before this process by going to the ms datalogger page and using the 'Save' facility.
Restore Defaults	:	All the default settings can be restored by clicking the 'restore' button. This facility can help in setting the master station and option modules to a known state before altering the settings for a particular system.
Configuration Files	:	The system configuration file can be saved by using the 'save' button. As default, the file will be named 'backup.nbb', but can be altered to a more meaningful name. It will be filed in a location chosen during the save routine. A previously saved file can be restored by browsing to the nbb file location and using the 'load' button.
FCU Tag File	:	The list of tag names for the field units can be saved by using the 'save' button. The saved file name is fcuconfig.xml as default and is filed in a location chosen during the save routine. A previously saved file can be restored by browsing to the file location and using the 'load' button. Modifications to the tag file can be made using a web browser and selecting the source view.

In some cases the web browser will open the fcuconfig.xml file instead of saving it. Save the file by using the 'save as' facility under the File menu on the web page. When naming the file, it will appear as fcuconfig_xml and the option of file type is presented. Ignore the options and change the file name and extension to fcuconfig.xml, then click on save. The resulting file will be in the desired xml format.

Update	: click on 'update'.
Firmware Update	: To update the firmware, browse to the location of the new file and click on 'update'.
Upgrade Key	: If a new key code has been purchased (to enhance the overall system capabilities) the new code must be entered here. Type the code into the box and click on 'update'.

7.5.22 Network

Fig 81:   Ethernet Network Settings web page

This screen is only accessible to Administrator user level.

In order to connect the master station to a network there are several settings and IP addresses that must be set. If that network extends onto the internet then additional settings for the gateway and DNS servers must also be added. This page allows these settings to be made.

Network Settings

MAC ID	: The unique identifier for this hardware. The Media Access Control number is embedded in the master station Ethernet port.
DHCP	: The Dynamic Host Configuration Protocol setting allows the master station to use a fixed (static) IP address or a dynamic address which it collects from the server. In practice, a fixed Static IP is usually preferred.
Host Name	: This is the identity of the basic module used in the system for reference on the Ethernet highway. The default of Pakscan3 is generally acceptable and need not be altered, even if several master stations are on the same network.
IP Address	: The Internet Protocol address that uniquely identifies this master station. This will generally be allocated by the network system administrator.
Netmask	: The netmask is allocated by the system administrator and set here.

Gateway	:	When the master station is connected to a gateway or router onto the internet, the gateway IP address is entered here so that the master station and gateway can exchange data.
Primary DNS	:	When connecting to the internet, the Internet Service Provider (ISP) will have two server IP addresses that are needed by the system to complete the data routing. Usually, data is exchanged via the Primary Domain Name Server IP. The address is entered here.
Secondary DNS	:	The second IP address supplied by the ISP.

Controls

Save Settings	:	Any changes are not implemented until the Save Settings button is clicked. Changes to these settings will require a reboot of the system. The web page will prompt this.

7.6 Setting Up the Master station Configuration Using the Web Pages

This section describes some of the settings required to be made in the master station to be able to correctly commission the Pakscan system.

In order to set up the system by using the web pages, it is necessary to access the system from a computer. This can either be directly connected, as described earlier, or via an Internet connection. Once the computer is connected, it is necessary to log in to the system at Administrator level using the correct password. Systems are shipped with a default administrator username of **admin** and password of **admin**. See section 7.5.1 for details of the log in procedure.

Select **Admin** to go to the start of the system set up pages. See section 7.5.15 onwards for details of the options available on the Admin page.

Click on **Masterstation Config** to enter the main system configuration page - see section 7.5.17. Modify this page to set up the master station parameters by using the drop-down boxes for each parameter. Most default values will be suitable for getting the system started, though consideration should be made for every setting.

Once the settings for each section are as required, they must be downloaded to the master station CPU module. Click on the appropriate **save settings** button for the changes made, and wait for the web page to refresh before moving to the next task.

7.6.1   Masterstation Config - Modbus Address

The Modbus address for host communications is set on the master station configuration page. Change the Modbus address to match the desired serial communication and Modbus TCP address for access to the actuators on the current loop. The user may need to change both the option 1 and option 2 Modbus addresses depending on the system. The two Modbus addresses must not be the same and it is advisable to change the addresses from the default values. Care should be taken to ensure that in a system with P2 (current loop) and P3 wireless option modules, the P3 wireless address will not conflict with the P2 Modbus address range i.e. in a system with 180 P2 wired devices the P2 Modbus address range will be the address set for P2 Modbus address + 2, therefore the first address available for the P3 wireless Modbus address will be the P2 Modbus address + 3. In a mixed system Option 1 will be the P3 wireless network and Option 2 will be the P2 current loop network.

The FCU distribution bar must be set up correctly to ensure that communication to all devices is possible.

7.6.2   Masterstation Config - Pakscan 2 Current loop option

The master station configuration page is also used for setting up the Pakscan 2 Current Loop option module if one is fitted. Set the loop performance parameters in accordance with site requirements. Make sure the loop speed is compatible with the value of the loop capacitance, see section 2.1.

❑ Set the highest field unit address parameter equal to the actual highest address.

❑ Doubling can be set to 'On' if the loop performance is not fast enough. It has the effect of halving the time to collect data from the field units.

❑ DV Convert should be set to 'On' if analogue position control is being used on the IQ, IQT, Skil or EH actuators on the network.

❑ Data Retain set to 'Off' clears all the field unit data if communication is lost. Some host systems want the data to be retained, in which case set the parameter to 'On'.

❑ Select the desired host database type for each serial communications port and the Ethernet ports for access to the actuators on the current loop. Refer to document PUB059-003 (formerly S171E) for database details. On Hot Standby systems link the alarms if both serial ports go to the same DCS or PLC in a redundant communications configuration.

7.6.3   Masterstation Config - Pakscan 3 Wireless option

If a wireless module is fitted, the master station set up page is also used for setting up the Pakscan 3 Wireless Network. Set the network parameters in accordance with the network settings recommended during the sire survey.

❑ Set the PAN ID and AES key as chosen by the customer.

❑ Set the channel number as determined by the site survey.

❑ Set the lowest FCU address to the lowest address in the range of addresses possible for the wireless module, avoiding overlap of addresses.

❑ Set the number of FCU addresses to the number of field units to be connected to the network.

7.6.4   Host port settings

The physical parameters relating to the serial ports that may be altered are set by accessing the **Host Port** page see section 7.5.18.

The port type is determined by the DIP switch settings on the main chassis behind the PS710 CPU module and the setting is reflected in the message on the screen. The description changes to reflect the settings made. This is particularly useful when determining the settings already in place. In hot standby systems the Cross Connected status of both the serial ports also depends on the settings of the DIP switches behind the Key Switch module on the main chassis.

❑ For each serial port, set the Baud rate and Parity as required. The speed may be varied between 2400 and 115,200 baud, the parity may be Odd, Even, Zero or None.

❑ On hot standby systems the Standby mode will normally be correct, when cross coupled, ports should be Standby Passive.

❑ On hot standby systems the Ethernet port needs to be set Standby Passive if both Ethernet ports are on the same Ethernet highway to the DCS. If there are two routes to the host they may be set Standby Active.

For security, IP Authentication should be set to the IP address of the Modbus TCP host(s). On a private network it is unlikely that authentication will be required.

7.6.5   Network IP address settings

The IP address for web page and Modbus TCP communication is set on the **Network** page.   See section 7.5.22.

The MAC ID for each Pakscan 3 CPU module is unique and fixed at time of manufacture. The IP address and Netmask (subnet mask) can be altered to suit the individual application and match the needs of the network.

Note: When the IP address is changed, the comms link will fail when the new value becomes active in the master station following the master station reboot. The web browser must be restarted and directed to the new IP address.

> *Re-establishing Ethernet Communication with a new IP address:*
> *Because most computers associate a MAC ID to each IP address, it is possible that the computer will not be able to re-establish communication with the master station until the computer has been rebooted.*

(This page is intentionally blank)

8. MAKING THE SYSTEM WORK

> ### *Always ensure the plant is in a safe condition and all the actuator controls are placed in Local before commencing any commissioning or fault finding on the system.*

8.1 Commissioning the Wired System

The current loop needs to be commissioned to enable the system to locate and identify every actuator. The master station and computer can be used to perform the commissioning. At the time of commissioning the loop, all the actuators must be made available, though they may be locked in 'hand only' control. All field units must have a unique network address.

The 2-wire loop and all the actuators should be connected to the master station, with all the actuators left without power, except for the one furthest from port A. Disconnect the wires from port B and browse to the master station web pages on the computer; go to **System Diagnostics** page – see section 7.5.4.

Select **Option 2 Diagnostics** by clicking on the **diagnostics** button - see section 7.5.7.

Reset the network (current loop) by clicking the **reset network** button. The status information will change and show the configuration stages. Once complete, the actuator furthest from port A should be shown on the Network Map.

Power on the next nearest actuator to port A and reset the network again. This actuator should appear on the list. Continue to power on the actuators and reset the network working back towards port A until all the actuators are connected and appear on the map.

Now connect the port B wires and disconnect the port A wires. Reset the network and check that all the actuators are still on the map. Having verified the loop wiring and the connection of all the actuators in both directions; finally reconnect the port A wires, reset the loop and all the actuators will be ready for control.

The commissioning sequence can also be carried out using the master station HMI screens using the Option Module 2 Diagnostics. This is a 2 page menu and contains similar information to the web page.

Once the system is working with actuators connected and no loopbacks present, the diagnostic and control pages can all be used.

See also the Quick start guide document: PUB059-026.

8.2   Commissioning the Wireless network

When an actuator with a wireless module is shipped from the factory, it will be set with default values for its PAN ID (Private Area Network Identifier), Channel number, AES (Advanced Encryption Standard) Key and Address.

These default values are:

- PAN ID   DA 15
- Channel   22
- AES key   0F 15 71 C9 47 D9 E8 59 0C B7 AD D6 AF 7F 67 98
- Actuator wireless module Address   300

These settings can be changed at the actuator using an infra-red setting tool or when communication has been established with the master station using the master station web pages / HMI. The actuator's wireless address cannot be set using the master station and must be set using the infra-red setting tool; each actuator must have a unique address.

It is best practice to setup the network such that the lower numbered devices are closest to the coordinator. This is because the reset of the network has been set up to be staggered, allowing those devices nearest the coordinator to join first, and more remote to join later.

At the start of commissioning the wireless network, leave all the wireless actuator modules powered down, power up the master station and set the desired PAN ID and AES key. These are to be decided by the customer. Set the channel number to the one determined during the site survey. It is recommended that at least the PAN ID is modified from the default setting. This will simplify commissioning by ensuring that actuator modules only appear on the network when the correct PAN ID has been set locally in them.

The PAN ID, AES key and channel number of the network can be set in the master station using the HMI screen or using the master station config web page.

Once the master station has been set up, the wireless actuators can be powered up and set up with the infra-red setting tool. If the master station settings are different from the default (as recommended) none of the modules will appear at the master station. At the actuator, the address should be set first then the PAN ID and the AES key. Refer to PUB002-008 for details of how to find the settings.

When these have been set up correctly, the new device will appear on the master station FCU menu page. It is preferable to set up the actuators one at a time, starting with those devices closest to the coordinator and working outwards to the unit furthest away.

See also the wireless quick start guide: PUB059-004.

8.3 Monitoring and Controlling the Actuators from the HMI or web pages

The web browser and HMI include the capability to control and monitor all the actuators on the Pakscan network. This assumes the actuators are in remote mode and correct permissions have been set up in the master station config web page – see section 7.5.17.

Using the web pages, go to **FCU Menu** to open the page showing all the connected actuators and their status – see section 7.5.11.

This screen lists the FCUs in address order, their type and current condition. The **FCU Control** button will bring up the page showing the information in more detail – see sections 7.5.12 onwards.

The actuator can be moved by the **Open** and **Close** buttons and any alarms present can be displayed by clicking **Show Alarms**. The page will automatically refresh if the valve is moved. The buttons at the top of the page can be used to move to the next or previous actuator on the network.

Control and monitoring can also be achieved using the master station keypad and screen. Select Field Unit Menu and the connected field units will appear in turn.
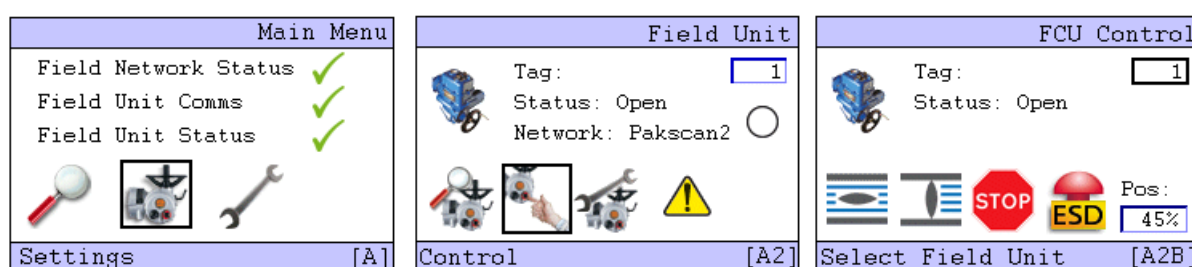

Fig 82:   *Detailed Actuator Condition HMI pages*

Once the system is running correctly, make a note of all the settings and field unit parameters for future reference.

The Pakscan Current Loop network and associated actuators will now be available for the host DCS or PLC to control and monitor the plant.

(This page is intentionally blank)

9.   LONG TERM DATALOGGER (LTD)

P3 master stations, delivered after May 2011, will contain a Long Term Datalogger (LTD) module. In the case of the hot standby master station, the LTD and the key switch are contained in the same module. For a single channel unit the module will be in the middle slot, which previously contained a blank module.

Fig 83:   Hot standby master station with Long Term Datalogger (LTD)

The LTD independently captures and stores all messages directed to the master station from the host connections and all the messages that occur between modules connected on the master station back plane. This information includes host Modbus commands and changes in field unit status information.

Information is stored on a microSDHC (Secure Digital High Capacity) memory card located at the front of the module for easy extraction. A 4 GByte memory card is supplied as standard. One file is created on the memory card for each day. The size of each file is dependent on how often the master station is accessed by the host. In practice, each day file is generally about 1 MByte.

The data is viewed on an application called LTD Viewer, which can be downloaded from the Rotork web site.   A memory card reader is required to connect the memory card to a computer to enable the data to be viewed.

The information monitored and recorded by the LTD can be saved for future reference and gives total visibility of every command and status update for every Pakscan device on the network. This information can be used by site engineers as part of their asset management function.
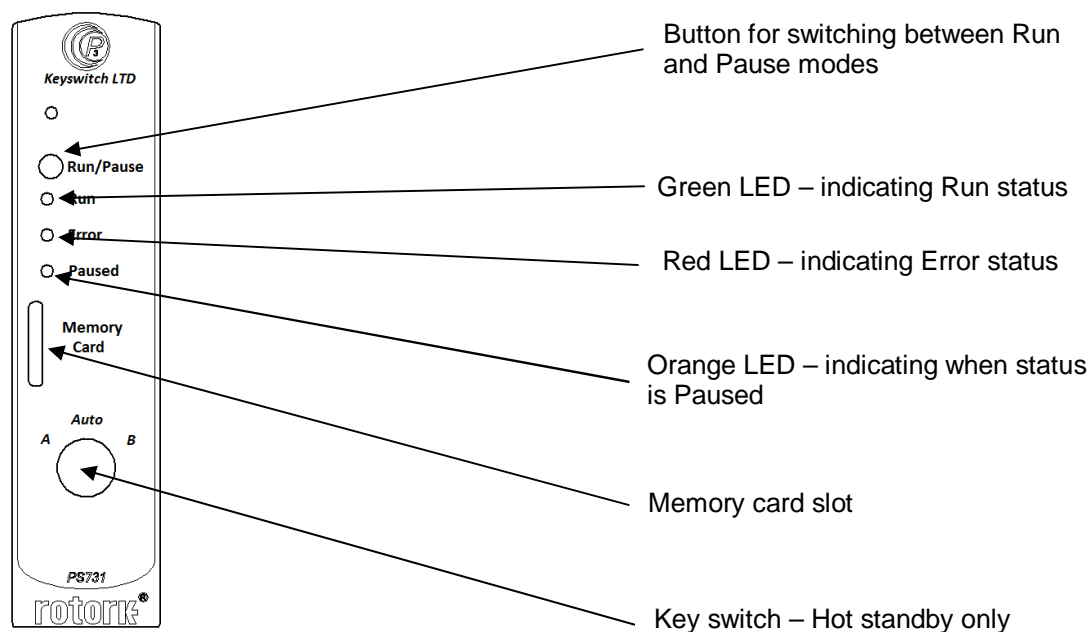
Fig 84:   Front view of the LTD

9.1 Removing the memory card and copying data

Before removing the memory card it is necessary to stop the LTD from logging. Press the 'Run / Pause' button once; the orange 'Paused' LED will start flashing. Once it has stopped flashing and is solid orange, it is OK to remove the memory card. This is achieved by pressing lightly on the card then letting go - the card should pop out enough for you to grab it. The card can then be placed in a card reader or USB carrier for extraction of the files into a computer. The card will contain the LTD Viewer software and also a folder with data inside:
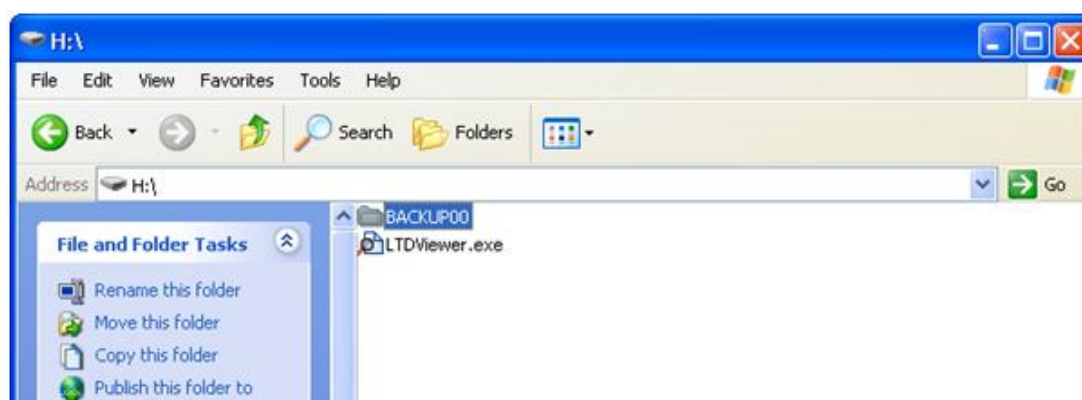
Inside the data folder will be a number of files containing the logged data, these files are not readable using a text file reader as they are in a Binary format.
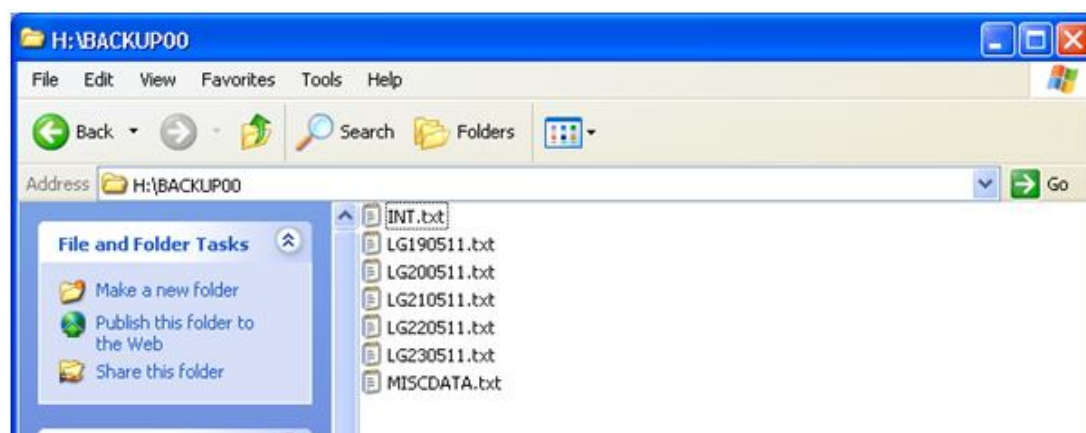
Each file is date stamped i.e. LG210511 is from 21st May 2011.

The complete data folder and the viewer software should be copied into a computer for viewing. The data folder can be renamed appropriately. Once the files have been copied from the memory card it can be replaced back into the LTD module. It should be replaced in the same orientation that it was removed (metal contacts to the left), gently push into place – it will click to indicate correct placement. If the card remains in place when pressure is removed then it has been successfully replaced. Once the memory card is back in place, the 'Run / Paused' button should be pressed once again and the datalogger will continue to log – the Run LED will flash Green.

It is important to handle the memory card gently when removing and placing the card in the module.

9.2 Viewing the data with the LTD Viewer software

The LTD Viewer software is started by double clicking the icon.
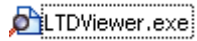
The software will open with this following page:
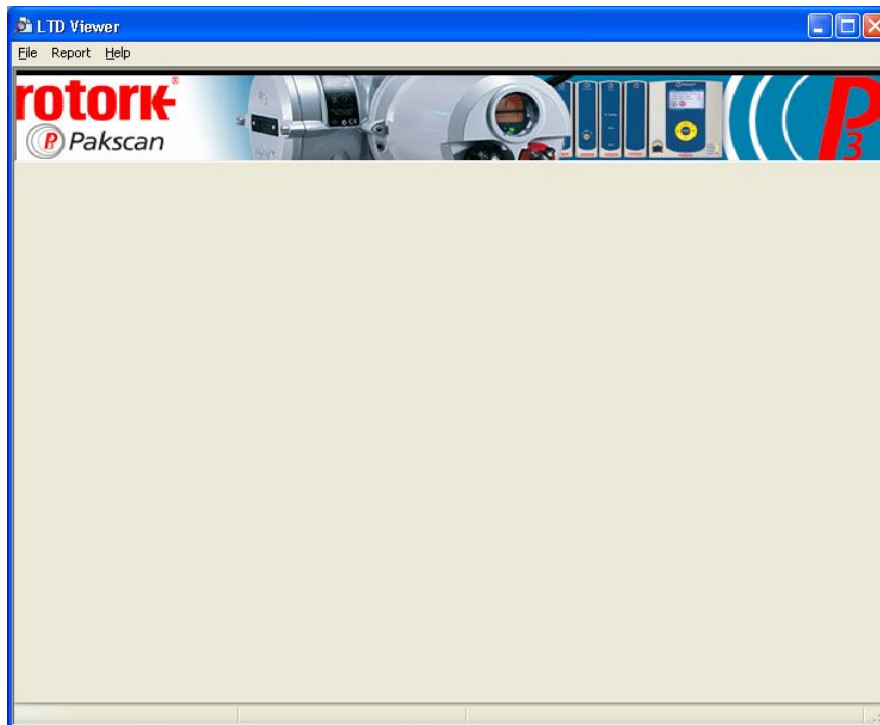
Click on File, then 'Select Folder', navigate to the folder containing the datalogger data.

Using the radio button select either 'Message' or 'FCU' to view the all the messages recorded by the LTD or the FCU data.

9.2.1   Messages

When 'Message' is selected the following page will be displayed:

From here the user is able to filter the messages in the datalogger. The datalogger records all messages that appear on the back plane of the master station including messages between the CPU module and the option card and in a hot standby system, the messages that are passed between each master.

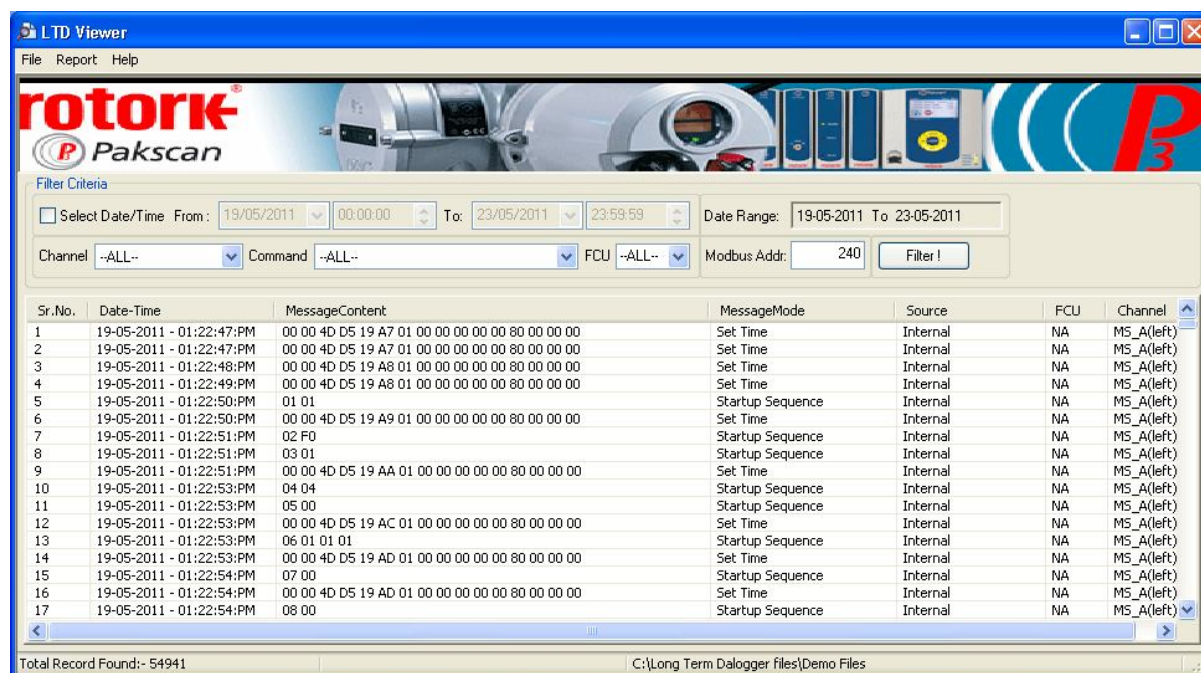The Date Range field shows the range of data that is held in the files. In this example we are able to see data in the datalogger between the dates of 19th May – 23rd May 2011.

9.2.2   Messages – Filter Options

It is possible to filter the messages to pinpoint the exact view you require. After each selection it is necessary to press the 'Filter !' button for the selected filter to take effect.

By selecting the 'Select Date / Time' check box, the user is able to restrict the data that is viewed between 2 dates. The date range is changed using the drop-down boxes and to update the data the filter button must be pressed:

In a hot standby system the user can filter on the A or the B side of the master station to only view data sent to the side selected:

The user can filter on a particular command or event:

The data can be filtered on the FCU address using the FCU drop-down box.

The data can be filtered on the Modbus address:

For example: to see all Modbus messages for all the FCUs on the A side of a hot standby master with Modbus address 240 between 19th May and 23rd May, the following filter would be set up:

Example data:

The data is displayed in a number of columns with the following headings:

- ❑ Sr.No: this is the serial number of the information within the display.

- ❑ Date – Time: Date and Time of the event / message.

- ❑ MessageContent: shows the complete message content i.e. complete Modbus message.

- ❑ MessageMode: shows the type of message and decodes it where possible.

- ❑ Source: indicates where the message came from and, for Modbus, which database is being used.

- ❑ FCU: The address of the FCU which the message is aimed for.

- ❑ Channel: indicates which side of the master station the message appear on.

There is a lot of internal status data passed on the back plane which is decoded by the LTDViewer. For example, in the command drop-down box, selection of Parameter Block Transfer and selecting 'Filter !' will enable these internal status messages to be seen. A lot of useful information is in there including status of the standby master station.

In this example we can see the position of one of the FCUs being reported.

9.2.3   Reports

If the user requires a report of the data in CSV / xls or html format, select the 'Report' menu item and then 'Messages'.
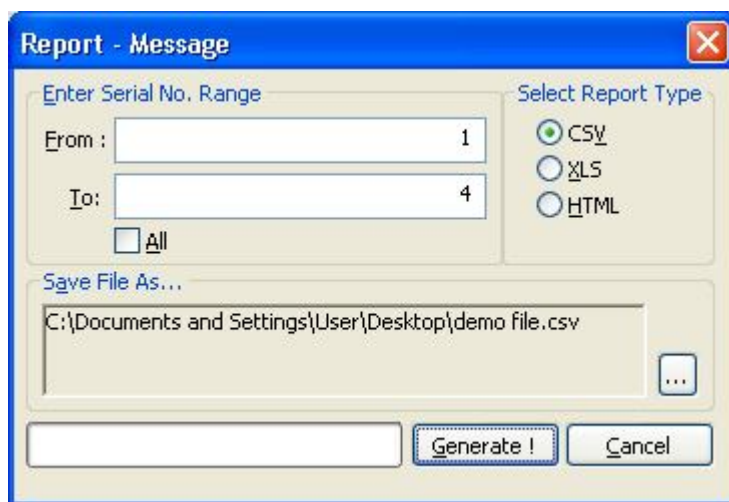
In the message box that appears select the range of data that is required – the range field uses the serial numbers i.e. in the example above there are only 4 lines of data so the serial numbers for those are 1 to 4. Click the 'All' radio button for all the data.

Select the format required and select a file name.

Select the 'Generate !' button and a pop-up box will appear to indicate success of generation.

The data can then be viewed in the chosen format i.e. CSV:

9.2.4 FCU Data

Select the 'FCU' radio button and then 'OK' to view the FCU data.
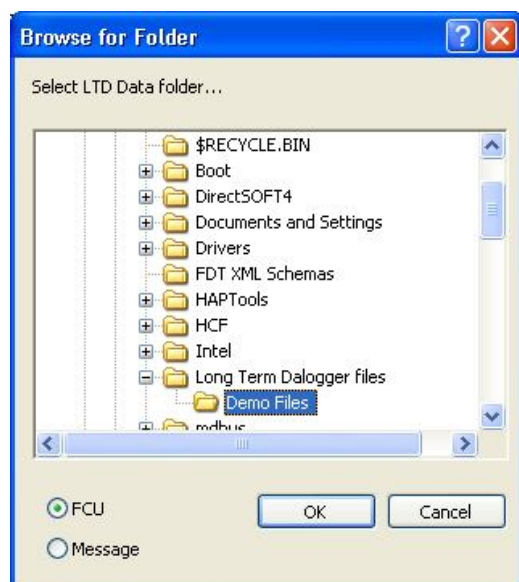
The FCU data page shows which devices are connected to the network and to which side of the master station they are connected. Here we have 2 devices; one is an IQT at address 1 and the other an IQ analogue card at address 61. Both are connected to the master CPU on the left hand side of the master station:

10. RESETTING THE MASTER STATION TO DEFAULT VALUES

> ### *It is important that anti-static precautions are observed whilst performing this operation.*

This section details how to reset a P3 master station CPU module to default settings using the hardwired link which is on a circuit board in the CPU.

❑ If the CPU module is part of a hot standby unit and control of the network is required during this process, use the key switch to force the 'other' side of the master station to be the primary unit.

❑ Isolate the power to the master CPU module that requires defaulting.

❑ Remove all connectors plugged into the CPU module.

❑ Remove the CPU module. For this operation the module removal tool supplied with the master station should be used to detach the master station from the back plane. The module is then removed by pulling it down and out from the back plane, then unhooking the hooks at the base of the module from the back plane.

❑ When removed, the default link is visible from the underside of the module, shown circled red in the picture below:

❑ The 'handbag' link will be across the 2 pins (of the 3 pin connector) furthest from the edge of the board.

❑ Carefully move the handbag link to the position shown below, such that it is linking the 2 pins closest to the edge of the board:

❑ Replace the module on the master station back plane and power up the module. Note: for a hot standby system, if the copy settings have been enabled when you replace the module you may find that the module re-boots more than once whilst the settings are copied across from the primary unit. Leave the unit powered-on for at least 5 minutes.

❑ Isolate the power to the same master module again.

❑ Remove the master CPU module and return the link to the standard position, as shown below – It is imperative that this is done:
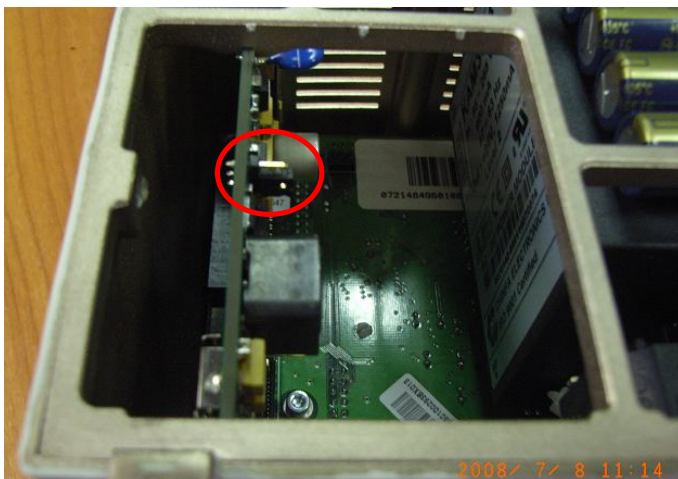
❑ Replace the CPU module on the master station back plane and power up the module.

❑ If the system is a hot standby, reset the switch to the auto position.

10. REPLACING THE P3 MASTER STATION BATTERY

> ### *It is important that anti-static precautions are observed whilst performing this operation.*

The Pakscan P3 master station has a small battery fitted in each PS710 CPU Module. This battery maintains the internal clock. The battery type is a CR1220 a 3 volt coin cell and should be replaced with a similar type of cell. Take anti-static precautions when attempting this procedure.
You can check the voltage of the battery by removing the PS710 CPU Module from the master station backplane. Then use a multimeter to measure the voltage between the battery holder (positive) and the end contact of J13 (negative), as shown in the picture below.

The battery should last about two years and should be replaced after this time as a matter of course. It should also be replaced if the measured voltage is less than 2.7 volts.

If the battery needs replacing, remove the seven cross-head countersunk screws and pull out the PCB support frame. Next, pull out the CPU PCB. Now carefully push out the battery and replace with a similar new part.

Replace the CPU PCB into the socket on the front panel PCB and carefully refit the support frame. Replace the seven screws and refit the CPU Module to the master station backplane assembly. Check and reset the clock if necessary in the CPU Module. Finally, dispose of the discharged battery in a suitable place.

GENERAL SAFETY INFORMATION

Customer information regarding installation, user safety, environmental and electromagnetic compatibility. This information is provided to assist with conformance to the Health and Safety Act 1974 and various directives of the European Community.

❑ **Mechanical**

The mechanical installation should be carried out as outlined in this manual and also in accordance with relevant standard such as the British Standard Codes of Practice.

Care should be taken to avoid dropping heavy items - for example during installation or maintenance. Protective footwear should be worn when appropriate. Rotork products are not intended to carry the stresses involved in support of items supplied by others unless this has been specifically agreed to by the company.

Care should be taken to avoid contact with sharp edges or points, particularly if the product is partially dismantled.

❑ **Electrical**

Products should be installed in accordance with BS6739 in the UK, or other appropriate local regulations for the country where installed.

Electrical supplies and earthing should be in accordance with BS7671 in the UK, or other appropriate local regulations for the country where installed.

Care should be taken to ensure that voltages or currents in excess of those specified, or of reversed polarity, are not applied to the terminals of any products. If such excess is applied, the product should be returned to Rotork or otherwise checked by a competent person before re-use, even if no damage is immediately evident. Use only the specified fuse type and rating as replacements.

Products should not be operated with safety protective covers removed, or with safety interlocks over-ridden. Some products are designed to allow access by skilled persons whilst power is applied. The user must control such skill level and access and it should be remembered that electromagnetic compatibility may be compromised.

Galvanically isolated input or output signal circuits are provided by certain products. A competent person must decide upon any earthing arrangements for such circuits and users should regard them as carrying a dangerous voltage, unless they are earthed locally.

❑ **Hazardous Area**

If the unit has a nameplate indicating that it is suitable for installation in hazardous areas then the unit may be installed in Zone 1, Zone 21, Zone 2, Zone 22 (for Div 1 or Div 2, Class I or Class II) classified hazardous area locations only. It should not be installed in hazardous areas with an ignition temperature less than 135degC. It should only be installed in hazardous area locations compatible with the gas groups stated on the nameplate.

The electrical installation, maintenance and use of the unit should be carried out in accordance with the code of practice relevant for that particular Hazardous Area certification.

No inspection or repair should be undertaken unless it conforms to the specific hazardous area certification requirements. Under no circumstances should any modification or alteration be carried

out on the unit as this could invalidate the units hazardous area approval certification. Access to live electrical conductors is forbidden in the hazardous area unless this is done under a special permit to work, otherwise all power should be isolated and the unit moved to a non-hazardous area for repair or attention.

❑ **Batteries**
Batteries must not be short circuited, or disposed of by burning. They must not be opened, punctured or crushed. Large batteries should only be used in well ventilated places. Their cases are generally ABS plastic resin and as such should be cleaned only with a damp cloth and not exposed to organic solvents.

❑ **Electromagnetic Compatibility**
To ensure conformance to the EC Directive 2004/108/EC, installation should adopt the following cable arrangements:

All digital data cables and all analogue signal cables operating at or below 50 Volts should be shielded either by braid, armouring or metal conduit. Such shields should be earthed at the point of entry to the product enclosure using cable glands designed for this purpose. If, for the avoidance of ground loops, it is not possible to earth these shields locally at low frequencies, they should nevertheless be so earthed via a capacitor effective at radio frequencies. If this technique is adopted, it is the users' responsibility to ensure that EMC is not compromised. A single shield may be shared by any number of analogue signal cables.

All Ethernet cables must be screened and of good quality. Many screened Ethernet cables of low quality have questionable screening efficacy.

❑ **Functional Reliability**
Reliability predictions, (including failure mode and effect analysis), are calculated by Rotork using statistical methods and the resulting figures should only be used for statistical purposes. These predictions are only valid if the maintenance procedures and maintenance intervals stated in Rotork documentation are observed.

❑ **Environmental**
Products should only be operated within the environment specified on the product data sheet. Take care not to obstruct ventilation paths.

In the event of ingress of any fluid or spray, products should be immediately switched off, and cleaned and dried by a competent person before re-use.

❑ **Chemical**
Specific hazards will be the subject of product data. As a matter of good working practice, oral contact should be avoided.

❑ **Independently Certified Products**
Such products must not be modified in any way by the user, and must be applied, operated and maintained in accordance with the relevant standards, certificates and reports.

❑ **Product Data Sheets**
These should be checked for information which supplements or replaces that given above.

❑ FCC Warning Statement
This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
> (1) This device may not cause harmful interference, and
> (2) This device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Contains Radio Module FCC ID: ZK4P3W-001.

Publication formerly known as S720E

rotork

http://www.rotork.com

Rotork reserves the right to amend and change specifications without prior notice.

Published data may be subject to change

UK Head Office

Rotork Controls Ltd
Bath
England
BA1 3JQ

Tel: +44 (0) 1225 733 200
Fax: +44 (0) 1225 333 467
email: mail@rotork.co.uk

USA Head Office

Rotork Controls Inc
675 Mile Crossing Blvd
Rochester
New York 14624
USA

Tel: +1 585 247 2304
Fax: +1 585 247 2308
email: info@rotork.com